# Messages that Motivate the Adoption of Safe Computing Behaviors

Kelline Greaves

July 5, 2017

University of Minnesota

School of Journalism and Mass Communication

Professional M.A. in Strategic Communication Capstone

Table of Contents

## Executive Summary

Cybercrimes are becoming more prevalent, sophisticated, and costly. Information security's technology interventions alone cannot stave off all cyberattacks. Rather, individual behaviors are instrumental to cybercrime prevention and self-protection. Research into motivating safe computing behaviors examine a range of strategies, including leveraging the health belief model, incentives, and persuasive communication. While the reviewed studies had promising results, no authoritative remedy emerged, suggesting that the method selected be tailored to audience. In addition, fresh research is required as the behavioral responses to cybercrime adapt and change to meet the challenges of rapidly changing technologies. This project intends to expand upon and advance safe computing persuasion research. Pursuant to the theory of planned behaviors, through focus groups, this capstone project seeks to gain insight into the attitudes, social norms, and behaviors of University of Minnesota employees in relation to safe computing behaviors. Attitudes that emerged among focus group participants included resignation, personal responsibility, practicality, and confidence. Several common social norms were also identified, including that people do not tend to talk about their safe computing behaviors with others; they tend to rely on businesses or organizations to safeguard their information, rather than taking personal action to protect themselves; when dealing with highly sensitive data, they follow required guidelines; and under normal circumstances people tend to perform some, but not all of the safe computing behaviors they believe that they should. Finally, perceptions of one's ability to perform safe computing behaviors varied among participants according to levels of confidence with technology, knowledge, and access.

In addition to applying the theory of planned behavior, this study also examines the efficacy of fear-based appeals in comparison to rational, confidence-building appeals in

motivating the adoption of safe computing behaviors. The majority of focus groups members indicated that fear-based messaging conveyed greater urgency and a more salient rationale to adopt the safe computing intervention, than did the more positive, confidence building message. While many preferred a positive tone, they felt it was less motivating. The insights gained from this research can inform messaging strategies used to persuade people to adopt safe computing behaviors.

## Introduction

Cybercrimes can have devastating political, reputational, financial, and psychological effects. Perhaps the most prominent example of cybercrime in headlines today is the phishing attack that allegedly enabled the Russian government to interfere with the American democratic process during the 2016 presidential election campaign. In part, the interference was made possible through the theft of former presidential hopeful Hillary Clinton's campaign emails which were then leaked to the press to undermine her credibility as a candidate. The emails were susceptible to theft because John D. Podesta, Clinton's campaign manager, gave up his username and password to a phishing attack that appeared to be a password reset notification. The information security breach led to a chain of events that, many argue, had direct impact on the election of Donald Trump (Lipton, E, Sanger, D & Shane S., 2016).

Another prominent example is the May 2017 "Wannacry" attack that installed ransomware onto Windows computer hard drives, essentially holding the affected device hostage until the owner paid money to the criminals. The computer owner's only alternative to paying the ransom was to wipe the hard drive clean, losing all data stored within. The ransomware leveraged a vulnerability in Microsoft's operating system, a problem for which there was a remedy. Only people who had not installed Microsoft's software updates were exposed to this threat (Lee, 2017).

A common factor in these scenarios is human behavior. In each case, criminals relied on people's failure to perform safe computing behaviors that would help protect them from attack. This assertion is supported by business leaders: "A recent survey of IT managers of global companies indicates that people remain the weakest link for information security in organizations..." (Van Kessel, 2008). Research studies have also found that users are not

adopting behaviors to safeguard themselves or their organizations (Boss, S, Galetta D., et. al 2009; Siponen M., Mahmood M., Pahnila. S, 2009).

Scholars who study cybersecurity and safe computing behaviors have sought to understand the nature and cause of this inaction in order that effective interventions and influence can be developed to increase awareness and adoption of safe computing behaviors. The body of literature on the topic is small in comparison to other areas of study as the academic world races to catch up with the speed of technological innovation. Recent scholarship is focused in the areas of cyber security awareness, attitudes, perceived behavioral control, motivations, and messaging. A survey of studies on affecting safe computing behaviors reveals conflicting opinions on the most effective approach. Some studies focus on incentives (external and internal), some believe that role models and organizational culture hold the key, still others look to influence through messaging. Because there are abounding audiences and disparate cultures, structures, and levels of awareness, and because there are ever-changing threats, ways to address them, and perceptions about efficacy or personal responsibility to safeguard one's self, there may be no panacea. However, if we are to curb the effects of cybercrime, it is valuable to understand the variables affecting persuasion, attitudes, and behavior. Therefore, this existent body of safe computing scholarship must be explored, validated, and expanded upon.

The study will apply insights from the literature and communications theories on fear-based messaging and rational, confidence-building messaging. In addition, focus groups will be convened with the intention of gaining insights into participants' attitudes, social norms, and perceived ability to conduct of safe computing behaviors. The purpose of this study is to advance the understanding of ways in which messaging can motivate the adoption of safe computing behaviors.

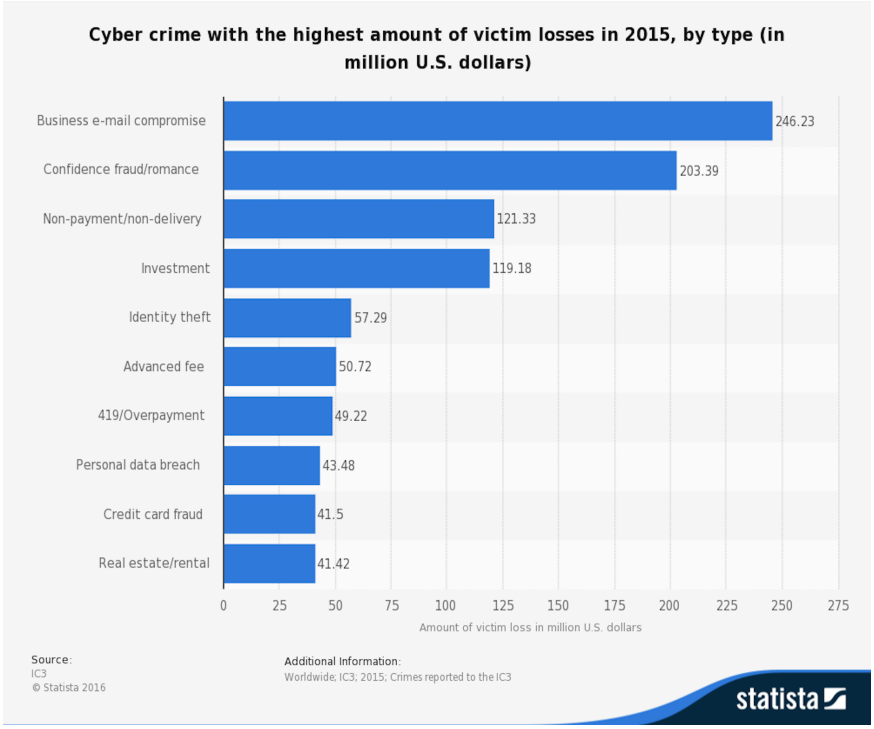
## Literature Review

Cyber security includes systems, policies, and behaviors designed to protect the data and integrity of computing hardware and software belonging to or associated with an organization or an individual. Cyber-attacks can include "Viruses erasing entire computer systems, intruders breaking into computer systems and altering files, intruders using your computer or device to harm others, or intruders stealing confidential information. The spectrum of cyber risks is limitless" (Cyber Incidents, 2017).

For the purposes of this study, safe computing is defined as a subset of cyber security dealing with the behaviors of individuals to guard against cybercrime. These include activities relating to protecting access to information, such as using strong passwords, using unique passwords for different accounts, using two-factor authentication, educating one's self on how to identify cyber scams, and updating software to ensure security patches are installed.

Globally, the costs to businesses are projected to top two trillion dollars by 2019 (Morgan, 2016). Costs to individuals are also being felt acutely. One form of cyber-attack is identity theft, a crime in which someone steals one's personal information, such as a Social Security Number, to commit fraud. A recent report shows that in America, victims of identity theft lost more than 57 million dollars (see figure 1).

**Figure 1**




Beyond the financial risk, there is also risk to one's well-being. "While the financial losses from identity theft are significant and the economic effects are far reaching, the socio-psychological harm to victims is incalculable. One police officer observed that identity theft can result in emotional and psychological trauma comparable to that experienced by victims of repeated physical assault" (Dadisho, 2005).

Cybercrime is increasing in frequency, breadth, and severity, but most people's defensive behavior is not adapting quickly enough. Therefore, research has been undertaken to understand and explain the lack of action by many to protect themselves from cyber-attack and ways in which to affect changes to behaviors.

**Health Belief Model**

Some researchers have looked toward the field of health and wellness as an analog to safe computing. This stands to reason, as in both subject areas, individuals are asked to learn and enact personal behaviors in order to prevent harm to one's self and promote wellbeing. The model was first developed in the 1950s by social psychologists who were working to understand the failure of a free tuberculosis screening program. The theory attempts to understand patient's reluctance to adopt preventive health behaviors as related to patients' beliefs and attitudes (Finfgeld, D. L., et. al, 2003, Rosenstock I.M., 1974). The health belief model constructs of susceptibility, perceived severity, cues to action and general health orientation are easily translated to information security. In applying the health belief model to the context of cyber security, researchers found that adoption of safe computing behaviors were increased when the subjects had better awareness about the particular cyber-attack (e.g., malware), understanding of the likelihood of the cyber-attack having an effect on the individual, and knowledge of interventions they believed would work and they were capable of performing (Dodel, M., & Mesch, G., 2017; Ng, B., Kankanhalli, A., & Xu, Y. 2009, Öğütçü, G., Testik, Ö M., & Chouseinoglou, O., 2016).

**Extrinsic Motivators**

Other researchers examined the efficacy of extrinsic motivators (e.g., pressures or rewards) as a means of promoting better safe computing habits. Research found that creating an external pressure in the form of a perception of mandatoriness had a positive impact on adoption of safe computing habits. Specifically, there was an impact in cases where subjects perceived that a behavior was required by management, that management could evaluate whether or not the behavior was performed, and where subjects believed that their compliance would be rewarded

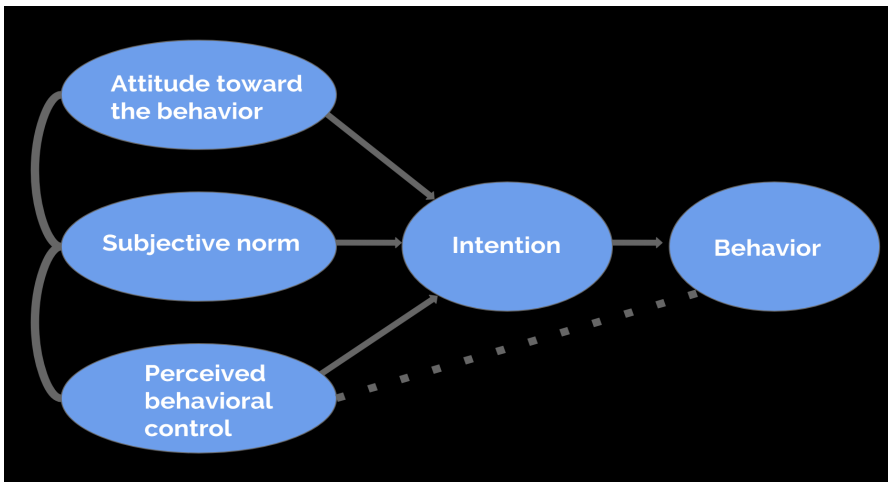
(Boss, S. R., Kirsch, L. J., 2009). Others found similar results regarding penalties and pressures, where penalties (perception that the organization would take action against a non-compliant employee), social pressures (perception that fellow employees will censure noncompliant employees) and the perception that the behaviors were effective had a positive impact on the adoption of safe computing behaviors (Herath, T., & Rao, H., 2009). Further, rewards for performing behaviors were found to be effective when accompanied with awareness training, and this measure had the added benefit of affecting a more positive perception of information security overall (Stanton J., Stam, K. et. al., 2004).

**Theory of Planned Behavior**

To gain further understanding into behavior motivation, we look to the theory of planned behavior (Ajzen, 1985). The theory asserts that intentions (indications of how hard people are willing to try, of how much effort they are planning to exert in order to perform a behavior) are the precursor to action. Intention is determined by three factors: attitudes toward the behavior, social norms, and perceived ability to perform the behavior.

Before one performs a behavior, one assesses what others are doing and makes a determination about what is acceptable or desirable (social norms), assesses the costs and benefits of conducting the behavior, and their ability to complete the behavior (perceived ability), and they form an attitude about the behavior. Based on these dependencies, one does or does not form an intention to act. Where there is intention, the behavior is more likely to be enacted (See figure 2).

Figure 2




**Function of Attitudes**

Attitude toward a behavior is a key component of the theory of planned behavior, and therefore, it is important to explore the concept of attitude more deeply. For this, we refer to the function of attitudes (Katz, 1960). This theory posits that attitudes perform four basic functions: utilitarian (seeking reward; avoiding punishment), knowledge (need to give structure to one's universe), ego-defensive (protects one from acknowledging truths about one's self or the world), and value expressive (demonstrating personal values and self-concept). The basic premise is that, if we can understand the function of individuals' attitudes toward safe computing behavior, we can design messaging that provides the appropriate stimulus for intention. For example, if individuals' attitudes about safe computing are utilitarian and reward seeking (either internal reward in the form of feeling proud of doing the right thing, or external incentives, such as receiving a coupon for a free ice cream cone) messaging should strongly promote the ease of taking action and the appropriate reward for doing so. On the other hand, if we assess that the attitude function is utilitarian and is seated in the avoidance or punishment, then the message should promote the ease of taking action, and emphasize the negative consequences of inaction.

**Persuasion**

Finally, since attitudes are so pivotal in determining behavior, we look to effective ways to influence them, specifically, we will evaluate the effects of persuasion. Persuasion can be defined as "a symbolic process in which communicators try to convince other people to change their attitudes or behaviors regarding an issue through the transmission of a message in an atmosphere of free choice" (Perloff, 2014). From Artistotle's *Rhetoric*, to modern scholars evaluating the communications tactics of the 2016 American presidential election, (Fitzduff, M., 2017, Steff, R., 2017, Dow, B.J, 2016), persuasion has been viewed as a powerful tool to affect attitudes, beliefs, and behaviors. Since this research aims to inform future study about how communicators might affect attitudes in order to motivate the adoption of safe computing behaviors, we will examine the efficacy of two forms of persuasion: fear-based appeals and rational/confidence-building appeals.

**Fear Appeals**

Fear appeals are messages designed to convey the seriousness of threat and the user's ability to cope with it (Johnston, A. & Warkentin, M., 2010). However, research has shown mixed results on its application. Where the fear appeal is extreme, and the information about how to respond to the threat is unclear, the result can result in a sense of fatalism and demotivation to act (Lawson, S, Haoran, Y. et. al., 2016). Others found that using protection motivation theory (Rogers, R. 1975) they were able to tailor a fear appeal that evoked a perceived threat that was both severe and likely to which there were effective, responses which people perceived they were capable of completing in order to drive intention and behavior. In these conditions, they found that fear appeals can be effective (Boss, S., Galletta, D, et. al., 2015). Still others tested interactive fear appeals which addressed the added element of flow, which describes an

absorbing state that people can enter when performing a task (Vance, A., Eargle, D, et. al., 2013). They found that interactive fear appeals had positive impact on users' creation of secure passwords, a foundational safe computing behavior.

**Rational, Confidence-Building Appeals**

Research has also been conducted to understand the persuasive impact of rational, confidence-building messaging. These kinds of messages appeal to rational cognition and positive confidence-building rhetoric rather than anxiety-evoking emotion to drive preventive behaviors. Rational messages build "self-efficacy, or confidence in one's abilities and in the safety measures used" (LaRose, R., Rifon, N., & Enbody, R., 2008). Other research asserts that hope (confidence-building) appeals can result in increased message attention, increased interest in the message topic, perceived message effectiveness, and behavioral intention (Chadwick, A, 2014).

In summary, the existent literature on safe computing behavior and communication theory, while enjoying some positive outcomes, support no definitive approach to influencing preventive behaviors. This suggests that the approach should be selected based on an understanding of one's audience. Therefore, the purpose of this study is to gain understanding of the University of Minnesota audience's attitudes, social norms, and perceived ability to perform safe computing behaviors, and to test the efficacy of persuasive messaging. This study will explore the relationship between fear-based and rational, confidence-building appeals and University of Minnesota employee intentions to take preventive action.

## Method

Focus groups are a strategy for understanding attitudes, opinions, beliefs and behavior in an "effort to collect preliminary information about a topic or phenomenon" (Wimmer, R. & Dominick J., 2010). Since the goal of this study is exploratory and seeks to understand the attitudes and behaviors of University employees about safe computing, focus groups were selected as the method of inquiry. The format of focus groups is a somewhat unstructured discussion between six and twelve people who are interviewed simultaneously by a facilitator.

Three 60-minute focus groups were held with University of Minnesota staff members during the week of June 19, 2017. Video and audio recordings were made of the conversations for future analysis. Focus group members were notified of the purpose of the study and were assured that their identities would remain anonymous. Weeks in advance to the focus groups, all participants were sent a consent form and immediately before the focus groups convened, were asked to sign and date them (see Appendix A).

During the focus groups, participants were asked questions about their perceptions, opinions, experiences, and beliefs about safe computing behaviors. In adherence to the theory of planned behavior, the questions were designed, at a minimum, to uncover attitudes toward safe computing and cyber-crime, perceptions of social norms, and perceptions of their ability to perform safe computing behaviors. In addition, in order to understand if the strategy of the appeal affected intention, participants were asked to react to examples of fear-based messaging and rational, confidence-building messaging.

**Institutional Review Board Approval**

Because this research project included human subjects, approval was sought and received by the University of Minnesota's Institutional Review Board on May 30, 2017.

**Recruitment**

Participants were recruited for the focus group by email invitation sent to University communications professionals, the researcher's colleagues, and via the researcher's personal Facebook account. No cash or gift incentives were offered. The selection criterion included only that participants be University of Minnesota staff members. Prior to the focus group, participants were encouraged to complete a short survey asking about their demographic information and their experience and perceptions about safe computing and cybercrime. Demographic information collected included age, gender, education, marital status and ethnicity. Questions designed to understanding of safe computing and cybercrime included:

- Are you familiar with the term "safe computing?"
- To your knowledge, have you ever received a phishing email (an email that appears to be from a legitimate business or person, but is really a scam that indents to steal private information)?
- To your knowledge, has your password, credit card number, bank account number, or social security number ever been stolen?
- How concerned are you about cyber-crime (crime that is perpetrated online?)
- How probable is it that you will be a victim of cybercrime?

The following tables indicate individual focus group member responses to the pre-focus group survey questions. The focus group member identifier number, found in column one, is also associated with individual participant comments (Appendix E).

Table 1

| Focus group 1 member identifier | Age range | Gender | Education | Marital status | Ethnicity | Familiar with term "safe computing?" | Have you ever received a phishing email | Has your password, credit card number, bank account number, or SSN ever been stolen? | What is your level of concern re: cyber crime | Probable victim of cybercrime? |
|---|---|---|---|---|---|---|---|---|---|---|
| F1-1 | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported |
| F1-2 | 35 - 44 | Female | Professional degree | Divorced | White | Yes | Yes | Yes | Slightly concerned | Somewhat probable |
| F1-3 | 45 - 54 | Female | Professional degree | Married | White | Yes | Yes | No | Slightly concerned | Not probable |
| F1-4 | 55 - 64 | Female | 4-year degree | Widowed | White | Yes | Yes | Yes | Moderately concerned | Somewhat probable |
| F1-5 | 35 - 44 | Male | Professional degree | Married | White | Yes | Yes | Yes | Slightly concerned | Somewhat probable |
| F1-6 | 55 - 64 | Female | Some college | Married | White | Yes | Yes | Yes | Extremely concerned | Somewhat probable |

Table 2

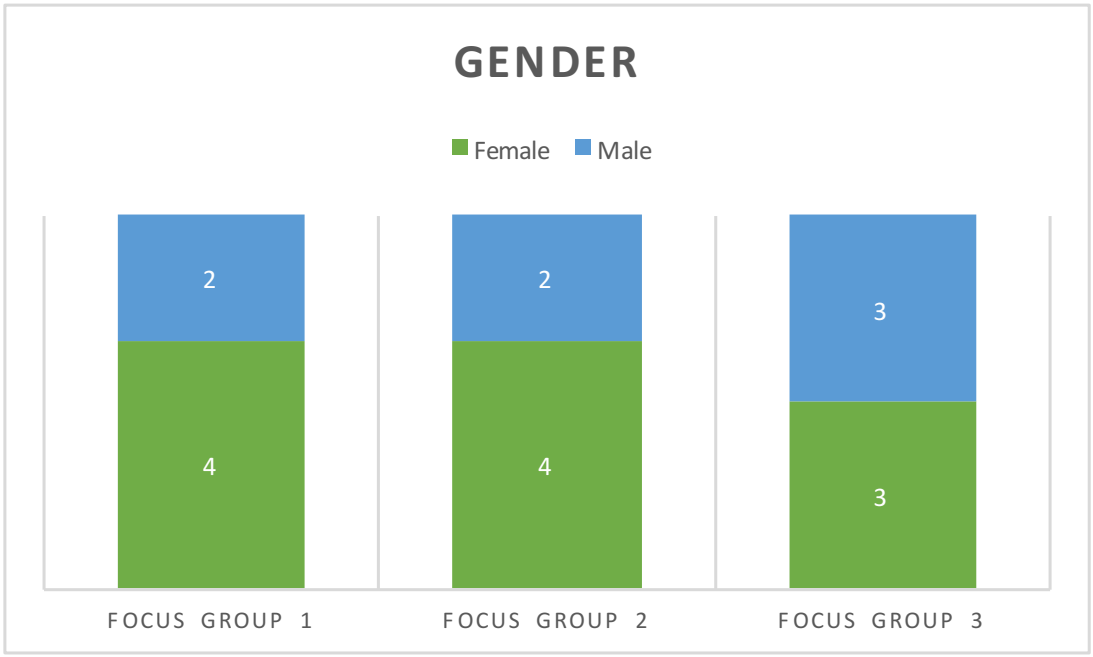
| Focus group 2 member identifier | Age range | Gender | Education | Marital status? | Ethnicity | Familiar with term "safe computing?" | Have you ever received a phishing email | Has your password, credit card number, bank account number, or SSN ever been stolen? | What is your level of concern re: cyber crime | Probable victim of cybercrime? |
|---|---|---|---|---|---|---|---|---|---|---|
| F2-1 | 35 - 44 | Female | 4-year degree | Married | White | Yes | Yes | No | Extremely concerned | Somewhat probable |
| F2-2 | 25 - 34 | Female | 4-year degree | Married | White | Yes | Yes | Yes | Moderately concerned | Neutral |
| F2-3 | 25 - 34 | Female | Professional degree | Married | White | Yes | Yes | Yes | Slightly concerned | Neutral |
| F2-4 | 55 - 64 | Male | 45 - 54 | Male | 4-year degree | Married | White | Yes | Yes | No |
| F2-5 | 25 - 34 | Female | 4-year degree | Never married | White | Yes | Yes | Yes | Extremely concerned | Neutral |
| F2-6 | 45 - 54 | Male | 4-year degree | Never married | White | Yes | Yes | Yes | Moderately concerned | Very probable |

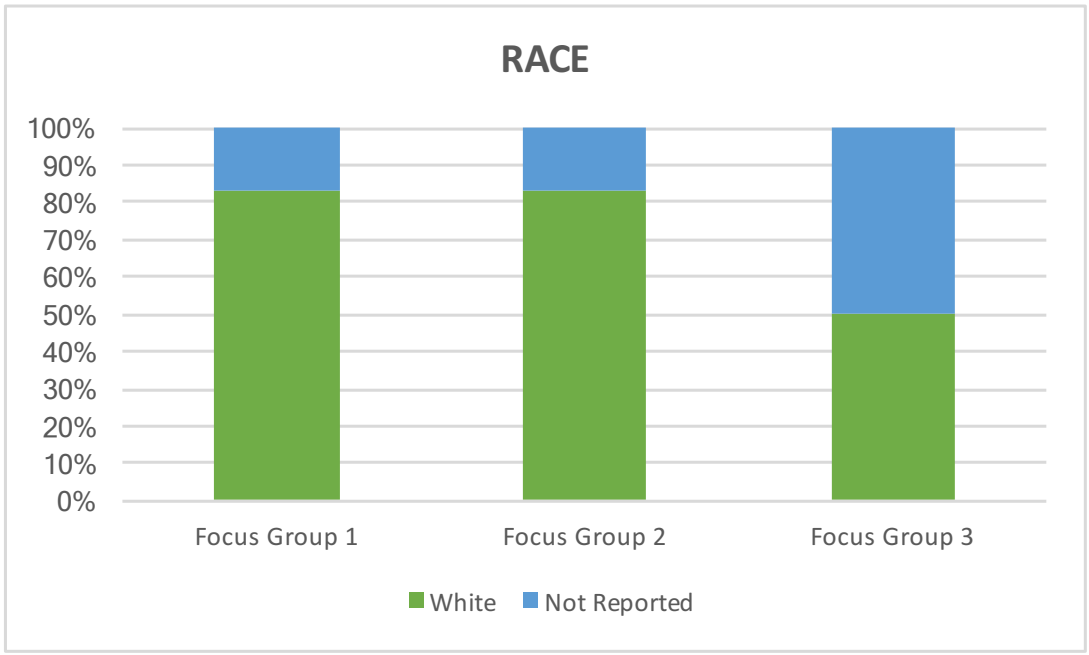
Table 3

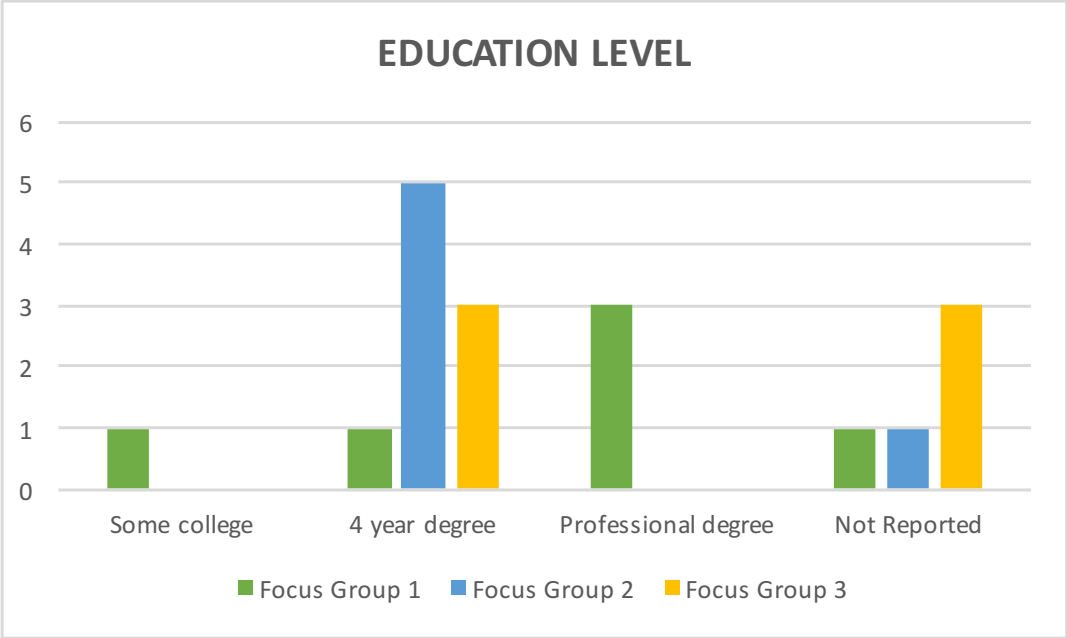
| Focus group 3 member identifier | Age range | Gender | Education | Marital status? | Ethnicity | Familiar with term "safe computing?" | Have you ever received a phishing email | Has your password, credit card number, bank account number, or SSN ever been stolen? | What is your level of concern re: cyber crime | Probable victim of cybercrime? |
|---|---|---|---|---|---|---|---|---|---|---|
| F3-1 | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported |
| F3-2 | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported |
| F3-3 | 35 - 44 | Male | 4-year degree | Married | White | Yes | Yes | Yes | Slightly concerned | Neutral |
| F3-4 | 35 - 44 | Female | 4-year degree | Never married | White | No | Yes | No | Moderately concerned | Not probable |
| F3-5 | 35 - 44 | Female | 4-year degree | Married | White | Yes | Yes | Yes | Moderately concerned | Somewhat probable |
| F3-6 | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported |

## Participants

Eighteen University of Minnesota employees participated in three focus groups (six participants per focus group). Thirteen of the participants completed the survey. The focus groups were formed based only on participant availability, rather than on demographic data or experience with safe computing or cybercrime.

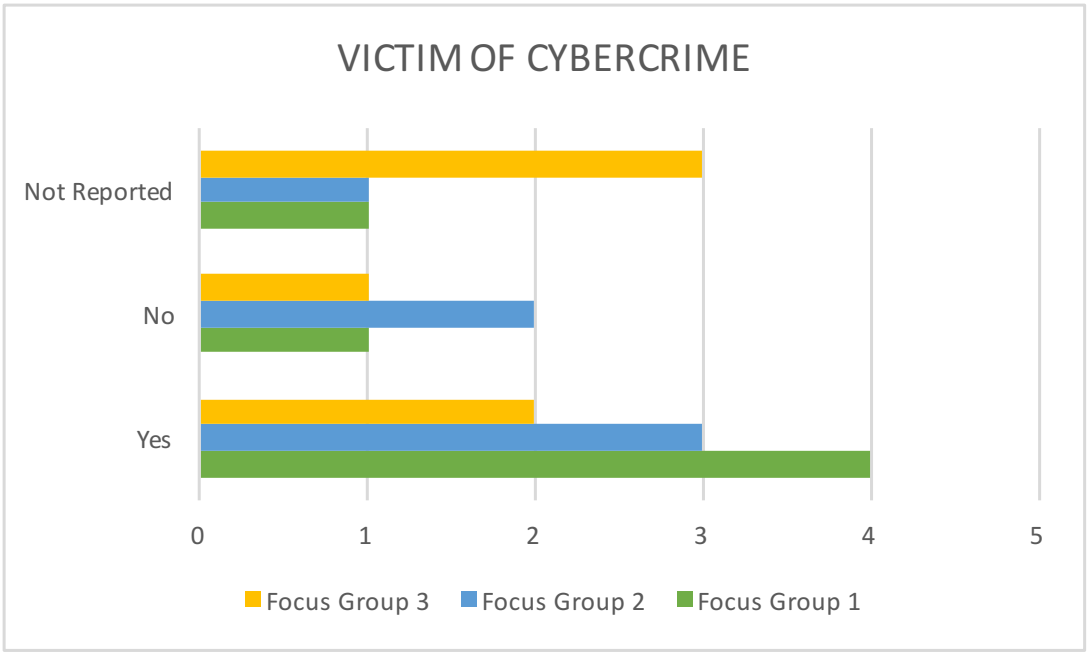

GENDER
Female
Male
2
4
2
4
3
3
FOCUS GROUP 1
FOCUS GROUP 2
FOCUS GROUP 3

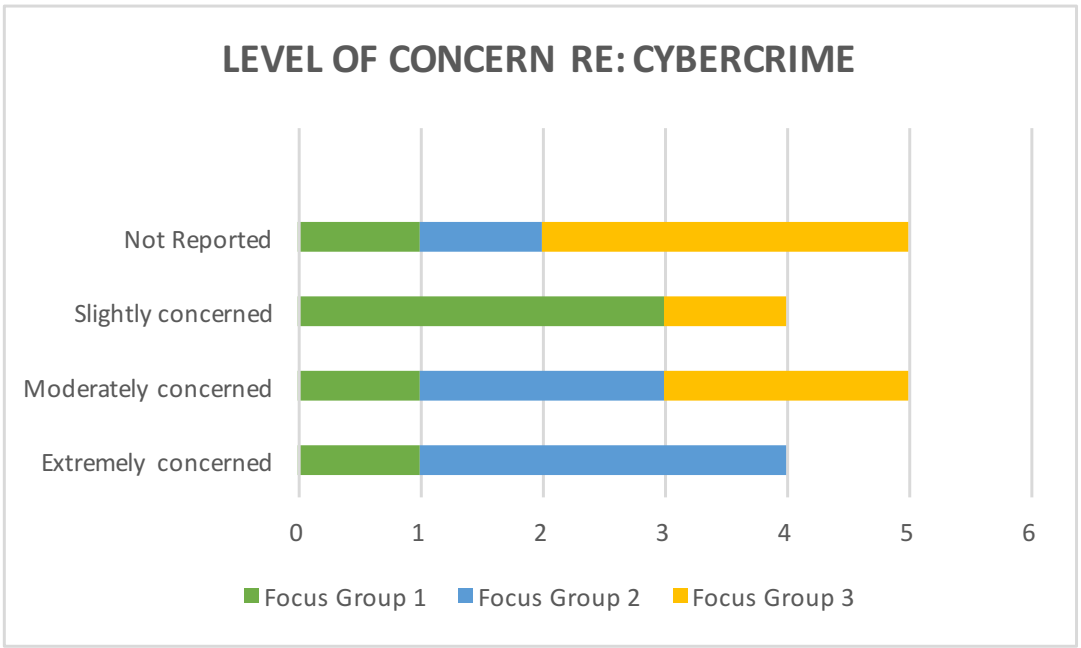

RACE
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Focus Group 1
Focus Group 2
Focus Group 3
White
Not Reported

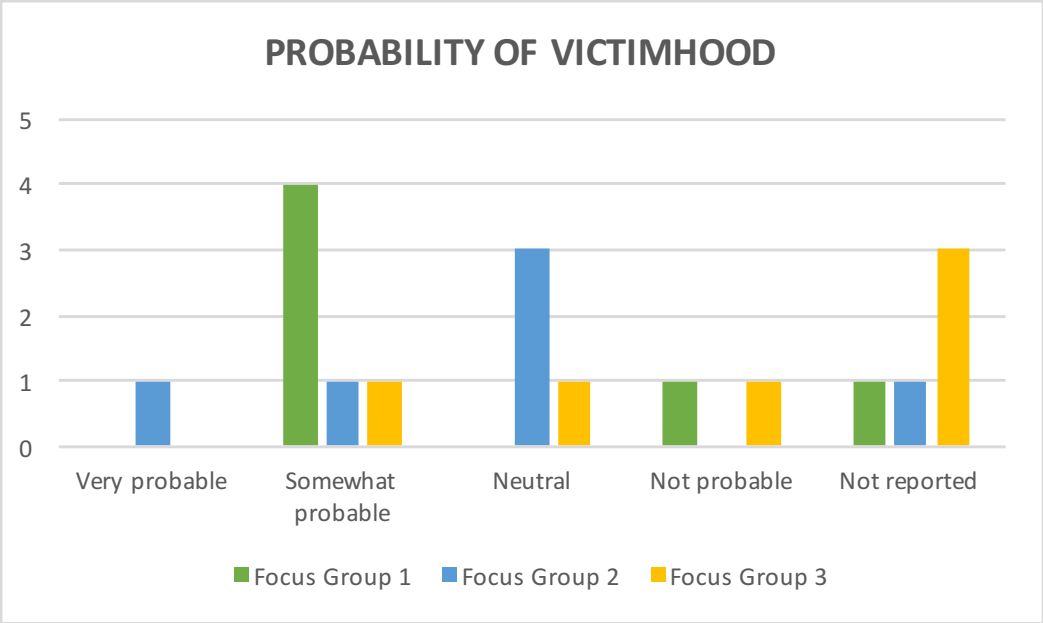



Demographically, there were more females than males, all who reported their race were white. Most participants reported having completed a four-year or professional degree.

In addition to demographic data, the pre-focus group questionnaire asked about participants' experience with cybercrime, levels of concern, and perceived likelihood of becoming a victim to cybercrime.


VICTIM OF CYBERCRIME
Not Reported
No
Yes
0
1
2
3
4
5
Focus Group 3
Focus Group 2
Focus Group 1


LEVEL OF CONCERN RE: CYBERCRIME
Not Reported
Slightly concerned
Moderately concerned
Extremely concerned
0
1
2
3
4
5
6
Focus Group 1
Focus Group 2
Focus Group 3




Of those who completed the questionnaire, 69 percent were moderately to extremely concerned about cybercrime (crime that is perpetrated on the internet); 50 percent reported that they had either had their credit card number, bank account number, or social security number stolen; and 53 percent expressed belief that it was somewhat or very probable that they would become a victim of cybercrime.

Note: In the following section, focus group members are identified by focus group number (F1, F2, or F3) and individual member number (1-6). For example, F2-4 indicates that the speaker was participant number four in focus group two.

# Findings

## Perceptions of Safe Computing

Following introductions and instructions for how to productively participate in the focus group (see Appendix B), the conversation began with a request for word associations with the term "safe computing." This exercise was designed to uncover participants understanding of safe computing concepts as well as to gain insights into their beliefs and emotions about the topic. Participants recalled several types of threats and common safe computing practices. Their responses demonstrated a good foundational understanding of the concepts around safe computing. Some of the conceptual terms offered by participants included: scams, back-ups, strong passwords, encryption, virus protection, antispyware, keeping things patched, virus, malware, phishing, malevolent links, and identity theft.

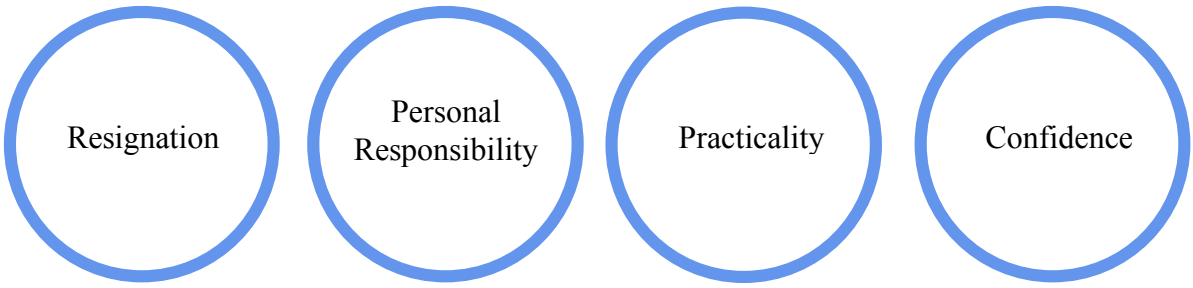
Participants also used descriptive words about their beliefs and emotions regarding safe computing. Their responses can be organized in three categories: **awareness of threat:** caution, exposure, concern, nervous, tiring, anxiety, and fear; **empowerment & self-direction**: vigilant, "protecting yourself," habits, "smart choices," "trying to keep ahead," "am I doing enough?"; and **resignation:** such as acceptance, "people will click on anything," "hope for the best;" and embarrassment.

These words provided insight into individuals' emotional and attitudinal disposition in response to the threat of cybercrime and the protective behaviors of safe computing. While all participants were aware that cybercrime was a threat, there were different reactions to it: some felt empowered to act, others felt disempowered and resigned to their fate.

In the theory of planned behavior, attitudes, social norms, and one's perceived ability to perform the behavior are factors that influence attitude and can help predict behavior. The focus group questions were designed to evoke responses that shed light on these three factors.

***Attitudes and Behaviors***

For the purposes of this paper, we will define attitude as a complex mental state involving beliefs, feelings, values, and probability to act in certain ways. During the focus group discussions, attitudinal themes emerged, including resignation, personal responsibility, practicality, and confidence.




Another emerging theme of import, though not an attitude, is one's relative interest in the topic.

Many participants expressed an attitude of resignation related to becoming a victim to cybercrime. The attitude was shaped by several factors, including the nature cyber-criminals, perceptions about one's attractiveness as a target, the nature of the internet, and one's past experience.

Over the course of the discussion, the groups covered cyber-attack tactics as far ranging as unauthorized access to one's accounts, identity theft, and email contact lists being hacked. People perceived cyber criminals to be both sophisticated and relentless. This sense engendered an attitude of resignation. Their comments implied that no safe computing measure would ever be enough to permit a complete sense of safety.

> "But, I just figure too, if my number is up, then so be it" (F2-4).
>
> "If someone really wants to read my email, they can probably read my email, there's not much I can do about that" (F1-5).
>
> "You're never safe" (F2-5).
>
> "You know it's like, at some point, I might get into a car accident. I'm always going to drive as safely as I can, but it's not always within my control (F2-3).
>
> "There are so many ways that it could happen that I don't know how to prevent it fully" (F2-5).
>
> "I guess I share a little bit of that feeling of inevitability. It's just trying to make it hard enough for someone to steal my identity so maybe they'll go after someone else. It's not a very charitable thing to do to the rest of society, but, I don't really know what else I can do" (F3-1).
>
> "I think it's a matter of time until they break that one [security intervention], and you just kind of stay ahead of it. I don't think that anything is perfect (F3-5).

The attitude of resignation to the status quo was also associated with one's perception of their attractiveness as a target. Some believed that because they do not stand out as a particularly interesting target for cyber thieves, (perhaps because they aren't extraordinary wealthy, they don't have access to desirable data, they are not public figures) that their risk is mitigated, and were therefore are not motivated to take action. When discussing his rationale for not using stronger or unique passwords, one participant said, "Part of me tells myself unless someone has a reason to target me. I'm one of billions of people that they could go at, so, I'll take my chances" (F3-2). Another remarked, "I take the attitude that I'm not that special" (F3-5).

With respect to online privacy, several felt resigned to the fact that their online habits were being tracked by corporations. "I am almost resigned to the fact that amazon knows everything that I might want to buy and that type of online awareness...I'm fine with that" (F2-2).

Additionally, participants expressed a sense of resignation based on their experience. One participant characterized her attitude as, "I've gone this many years without anything happening

to me, and then you just start to feel safe" (F2-1). While another focus group member felt that people's complacency was based on the experience of computing being an everyday behavior, like driving a car. "I don't think that people realize the consequences of getting into a car. It's one of those things that you have to do on a daily basis so you sublimate the risk factors" (F1-1).

Another attitudinal theme was personal responsibility (or lack thereof). Nearly all participants confided that they were not using all the safe computing measures they could. Encouragingly, one participant felt that with more knowledge she was motivated to take personal responsibility for safe computing at work. "I went to a safe computing workshop recently and after that, a coworker was working from home and G-chatted me, like 'Hey, can you log into my computer for me,' and I was like, 'I'm gonna call you!' and I felt very proud of myself" (F2-3). Others felt responsible only to adopt University required safe-computing behaviors. "I think I do all of the things that we're mandated to do" (F2-4). "We have Duo. That is what OIT says to do" (F3-4).

However, repeatedly, participants claimed no need to take personal responsibility to adopt some safe computing behaviors due to the practices of businesses to remediate the consequences of online theft. Regardless of their own online behavior, they feel secure. As an example, one participant stated, "My credit card number has been stolen multiple times and I always get a phone call and am always off the hook" (F2-3). Another stated, "I just have such confidence that if my paycheck were stolen, there would be some recourse for getting that money back" (F1-2).

Most participants felt that it would be more responsible to adopt better computing practices, but they were not compelled to do so. One person confided, "So, those are things that I know I could do, but for whatever reason, but for some reason, I haven't yet" (F2-2). In part, this may be explained by feeling overwhelmed, which has been shown to be demotivating, and can lead to

inaction (Lawson, S. T., Yeo, S. et. al., 2016). Several focus group participants, felt that beyond the relentless nature of cyber-criminals, the demands of safe computing were also overwhelming. In particular, when the discussion turned to learning about new scams, and learning about the latest in new passwords, people took the attitude that they could be personally responsible for only so much.

"It's a huge demand" (F2-6).

"I could spend all my day trying to keep track of all the passwords" (F2-4).

"I can only remember so many things" (F2-5).

Yet another prevailing attitude was that of practicality. Several focus group members contended that, while they would do what they could to prevent becoming a victim of cyber-crime, they would, as a practical approach to life, choose not to live in fear. "But then, I remind myself that we're not any more unsafe than we were 40 years ago. We just all know about it now immediately. I try not to live in fear" (F3-5). Another participant took the practical approach that he would put in more or less safe computing effort relative to the value of that which he was trying to protect. "If I had something that was so valuable to protect, I would lock it with a lock that was like $10. Then eventually, when it's worth more than $10, it's going to be worth it for them to go get it" (F3- 2).

Another attitude that emerged was confidence in one's ability to detect a cyber-attack. Participants displayed a range in levels of confidence regarding both themselves and others. Many thought that they could easily identify a scam. One participant stated "I think it just is intuitive to me" (F2-1), while another asserted, "I feel like I'm savvy enough" (F2-3). Some participants expressed lack of confidence in the abilities of those with less experience, saying "I feel real nervous about old people who don't understand the internet very well. They aren't as

concerned about clicking on links and downloading things and like "winning a prize" (F2-3). When contemplating why she does not use some safe computing technology, on participant stated, "I may be nervous that there is some technical piece that I don't know, and maybe that's why I'm not starting to...they can give me steps, but I can look at that and feel like I'm not quite sure I know how to do that, and then don't take action to find someone who can help me with it" (F2-2).

Finally, though not an attitude, it is important to note that level of interest in the topic of safe computing affected their behavior. For some, the topic of safe computing is dull, while for others it is of interest since it is part of their daily work. For those who expressed low interest, learning about safe computing practices and tools is a greater challenge. "The words 'Safe Computing' are so fundamentally sort of boring to me, that I'm not going to sign up for a service that is going to keep me up to date about that" (F1-2). One participant disclosed that her interest was piqued by "strong wording from central administration" and her own curiosity (F2-3). Another participant recommended that his interest might be sparked by introducing a "gaming mentality" (F1-1). A gaming mentality might include a competitive framework where one might earn points or rewards by performing safe computing behaviors, such as downloading two-factor authentication or taking a strong password training.

***Social Norms***

The next consideration in the theory of planned behavior is social norms. To understand social norms with respect to safe computing behaviors, the focus groups were asked questions relating to the safe computing practices and experience of their colleagues, friends, and family. They were also asked if they discussed cybercrime or safe computing with others and where they learned about new safe computing standards.

Several themes emerged including that groups don't tend to talk about safe computing, unless it's to say how frustrating it is; people rely on the University to keep them safe and to tell them what to do; when people have access to private information, they use appropriate precautions, and people tend to perform some, but not all of the safe computing behaviors they believe they should.


Several participants reported that they did not to talk about safe computing in their work spaces. Another stated, "I most often hear about passwords and how frustrating that is…That's the only conversation I have with people about this, unless something happens to them (F1-2). Yet another participant said that she did remark to colleagues when she changes her password, but that it only happens annually (F3-5). The limited (positive) conversations about safe computing make it difficult to establish positive attitudes and the perception of that the use of safe computing behaviors is pervasive.

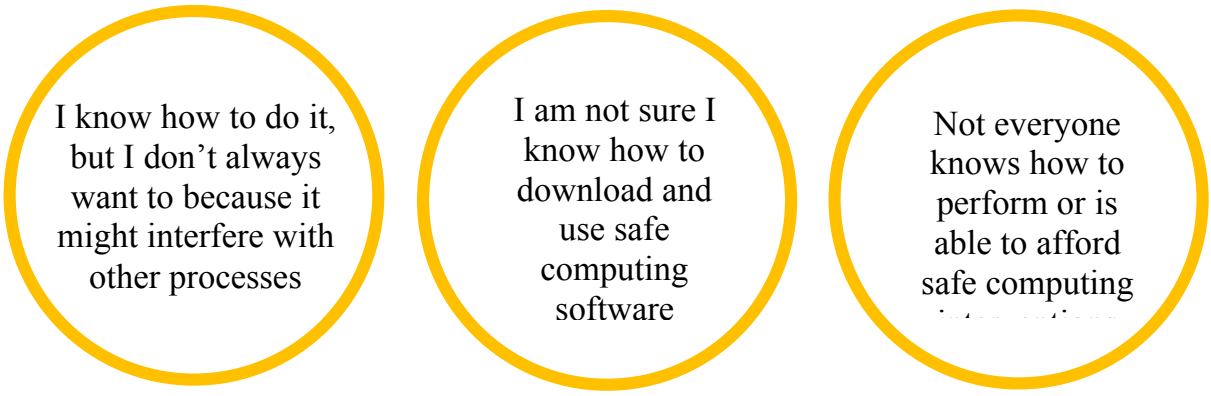
The second social norm that emerged was that people rely on the University to keep them safe and to tell them what to do. Rather than seek out information on their own, participants indicated that they rely on the Univeristy of Minnesota's central technology unit, the Office of Information Technology (OIT). One person stated, "I would say I don't think about it a lot until I read something or get a newsletter from OIT or something. That makes me think about it" (F3-5). Another participant observed, "I trust the U to keep us safe here" (F2-1). Generally, there was

a sense that if it were important for people to understand or do, the University of Minnesota would let them know.

A third social norm that emerged was that people who had access to protected or sensitive data took the appropriate steps to safeguard it. Several of the participants shared that they had access to University data that is classified as protected, which might include such things as student grades, personal health information, or employee data such as direct deposit accounts. Participants expressed that they adopted the use of two-factor authentication (some were required to do so, others were not) when they accessed data they knew to be vulnerable or valuable to protect. In addition to doing what is required by their jobs, there was both a sense of doing the right thing to protect the people who could be hurt by their data being compromised, and that of doing the right thing for the University of Minnesota.

***Perceived Ability to Perform Safe Computing Behaviors***

Another key factor in the theory of planned behavior is an individual's perceived ability to perform a behavior. Some key themes emerged during the focus group conversations.




Several participants noted a lack of confidence in their ability to effectively use safe computing tools, or adopt safe computing practices. One focus group member offered that

sometimes the perceived ability is not only about knowledge, but can also be about cost. “Not everyone has the know-how to (buy a private VPN service) or the money to pay for it” (F2-1). Some participants felt that they could perform the behaviors, but were reluctant to for either reasons they could not name or due to inconvenience. Several participants were skeptical and sometimes reluctant to perform software patches because of their sometimes-annoying side effects, such that the intervention actually affected their ability to work with technology. “Sometimes, (after a patch) things don’t work properly. Then, it’s like ‘Why can’t I print now?’ or whatever, and that is a big pain” (F2-6).

**Fear-Based Messaging Compared to Rational, Confidence-Building Messaging**

The second half of the focus groups were devoted to participant reactions to two different persuasion strategies: fear-based messaging and rational, confidence-building messaging. To that end, participants were asked to review two printed 8.5x11 flyers promoting a specific safe computing technology: Duo Two-Factor Protection for W-2 and Direct Deposit. Opting into Duo is the desired safe computing behavior promoted by the flyers. This example of a safe computing behavior was chosen because, like most safe computing behaviors, it is optional, it takes some amount of time and effort to enroll, and the potential consequences of not using the service are substantive.

Participants were instructed that the flyers were prototypes, and that the exercise was not so much about the design and layout, but that there was more interest in understanding how each of the flyers made them feel, what they understood to be key messages, and whether or not they found the messaging motivating. First, participants were given several minutes to review the fear-based flyer, referred to as “the wolf” because it shows an image of a wolf in sheep’s clothing, a metaphor for phishing emails (see Appendix D). They were invited to write down

thoughts and opinions as they occurred to them. A discussion followed. After that, the same process occurred for the second flyer which contained rational, confidence-building messaging. The second one is frequently referred to as "The blue one" because it's primary color was blue (see Appendix E).

### ***Reactions to Fear-Based Messaging***

Participants were asked for their impressions and key takeaways from the fear-based "wolf flyer." They were asked how it made them feel, and if they thought it was effective. Their responses are categorized here in themes: urgency and tone, efficacy of word choice, and compelling rationale.

#### *Urgency & Tone*

For the most part, participants found that the wolf flyer had a serious tone and conveyed a sense of urgency.

> "The (wolf) one creates a sense of urgency, or anxiety in general. (F1-1)
>
> "I thought the text struck a nice balance between not being overly dramatic…it's has a sense of urgency but doesn't seem to be going into the "sky is falling" The way that the vocabulary was used, not too dramatic not too wishy-washy. (F3-6)

There were exceptions, however. Two participants offered that, for them, word choice undermined the flyer's sense urgency.

> "The language 'set aside ten minutes' turned me off. It took away all urgency" (F1-6).
>
> "It says 'Opt into' rather than 'activate' Duo Protection - I associate it with something that is not urgent, like 'opt into our emails'" (F1-5).

These participants felt that if the promoted safe-computing behavior was optional and if it required them to set aside time to do it, it was not urgent, in spite of the stark consequences articulated within the flyer.

Some found the flyer's tone to be scary, which left them feeling overwhelmed. "It's a sobering tone, but it's also a little overwhelming. I think that the image is pretty stark and kind of scary" (F3-3). Others also responded negatively to the evocative flyer. For example, one participant felt it was a challenge to his abilities, "Would they (hackers) really get me?" (F3-1) and another felt that because the message was fear-based, it was condescending and meant for someone less savvy (F2-5).

*Efficacy of messaging*

There were also plenty of comments about the messaging itself. Some reacted positively to wording that reflected the difficulty of detecting phishing emails. "I'm glad it has the word 'sophisticated' because sometimes I read things like this and I feel like they're condescending, and I feel like I'm better than that" (F2-5). Others appreciated the instructions. "You could walk away and you have steps to do it today. There's a call to action." Another stated, [I like that it tells you that it takes ten minutes to enroll] "You're not going to have to take an hour" (F2-1).

*Compelling/Not Compelling Rationale*

Participants were asked if the contents would motivate them to take the desired action. They were asked to examine what were and were not compelling reasons to take action. Almost universally, people indicated that a stolen paycheck was more motivating than any other reason for opting into Duo Protection.

> If it is just about SSN and paycheck, I would flip the two. "You're a target for identity theft" I accept that, right? The paycheck is more of a threat (F1-5).
>
> I don't care about my SSN as I do about my paycheck (F1-1).
>
> I think the most compelling thing is 'am I protecting my paycheck?'...Seeing "paycheck" on here is like that is something I want to protect. Because we all know protecting our SSN is important but we don't think about the consequences of what does happen (F2-3).

Other's advised that sharing statistics would be motivating for them either regarding consequences like how long it takes to recover your paycheck, how many people were affected or how many had already opted in.

Several participants advised that altruistic or University-focused motivations would be effective. Several recalled the University of Minnesota campaign for getting flu shots, "Doing it for the herd" and thought it was applicable. "Like the herd mentality that you get for the flu shots. Like we're the herd. The U is the herd. Do it for the herd!" (F3-5). Another focus group member agreed, stating "You are kind of doing it for the herd, too, because you know, if someone on your network gets hacked, that can be your issue too. Or, if someone at the desk next to you clicks on some phishing thing, that compromises the server you're both on, that's an issue too" (F2-6).

The overall consensus was that the messaging about losing a paycheck was the most persuasive, but they were also interested in messages that reflect actual data that by using Duo, they were significantly reducing risk of dire consequences, and they wanted to know that the majority of their peers were also using the service.

***Reactions to Rational, Confidence-Building Messaging***

Participants were asked for their impressions and key takeaways from the rational confidence-building "blue flyer." They were asked how it made them feel, and if they thought it was effective. Their responses are categorized by themes of urgency and tone, efficacy of word choice, and compelling rationale.

*Urgency & Tone*

Generally, people found the tone of the blue flyer to be friendly and encouraging. Some appreciated this. One participant stated, "I don't feel like I'm being pushed as hard, or manipulated or made to feel scared by the way the message is being presented" (F3-3). Another added, "It has more of a tone like I'm your friend, I'm telling you what you should do. Duo is now my best friend because now we're together. And we're so happy in this picture. But it is less anxiety inducing than the whole scary wolf in sheep's clothing one" (F3-6).

Others felt that the tone came across as intended for someone who is not internet-savvy. "I think it's geared toward someone who is not in this room. If someone doesn't understand the problem at all. It feels like, I might send this to my mom...It's a little condescending" (F1-1). In contrast to the wolf flyer, which was more urgent and evocative, one participant compared the blue flyer to "Smokey the Bear" implying that it was a little childish in nature.

*Efficacy of messaging*

Some appreciated the way that the flyer characterized the threat. "I appreciated the if-then statement. If your password is stolen, then access to your accounts is just a few clicks away. So, it gives shortened consequences" (F2-3).

Another participant thought that the call to action wasn't strong enough. "[Where it says], 'You can help protect.' I would go 'protect your identity'" (F2-5).

*Compelling/Not Compelling Rationale*

Participants thought some of the provided arguments for opting into Duo were less effective than others. Again, people reiterated that "Phishing emails don't scare me. It's the second part [the paycheck], that's most important" (F2-5).

Others disliked the rationale of "feeling great." In the blue rational, confidence-building message, the content suggests that "you'll feel great knowing you have added another layer of security in front of your SSN and paycheck." One focus group member commented, "It diluted the call to action here. So that's the only reason (to opt in), is for "my great feelings?" (F1-2).

Some thought the effective messages included that the service was free. I appreciated that this said that U of M offers a free service. It's a little thing, but everybody loves free stuff (F2-3), and they appreciated that the messaging communicated a sense that the University cared for them, and that "with Duo, you can make a difference. Like we're in this together" (F2-3).

# Discussion

## Attitudes, Social norms, and Behaviors

The most effective messaging says what people want or need to hear in the way they want to hear it when and where they are ready to hear it. This study helps contribute to understanding how to maximize that equation for persuading people to adopt safe computing behaviors. Several attitudes that emerged from the discussions: resignation, personal responsibility, practicality, and confidence. Understanding these attitudes and their underlying beliefs or values will be useful both for future study and for formulating communications strategies.

Social norms regarding safe computing behaviors are not publicly visible or necessarily the topic of conversation among most people. The focus groups supported this assertion. In these discussions, unless information security is expressly a part of one's job, most conversations about safe computing are regarding how frustrating or inconvenient it is to perform them.

Generally, the focus group participants indicated that they were aware of what they should be doing, but did not adopt all of the behaviors they could.

## Fear-Based Versus Rational, Confidence Building Messages

This research found that fear-based messaging was more effective for motivating behavior. Participants perceived greater urgency and found that the rationale for adopting the safe computing behavior (opting into Duo) more compelling in the fear-based messaging. The emphasis for the fear-based messaging seemed to be more important for protecting one's self. Even in the case where people found the positive, confidence building tone to be more palatable, they thought the fear-based language would be more likely to motivate action. "I like the blue one better, but I'd probably be more likely to do something based on (the wolf flyer)" (F3-4).

The research showed that very few people cared about protecting themselves from identity theft, feeling it was too far out of their control. In the case of opting into Duo, they thought that loss of their paycheck was most consequential rationale.

There was a contingency of participants who felt that positive, altruistic messaging would be motivating. They liked the idea of doing the right thing for the University of Minnesota and their colleagues. They thought that engaged employees would find protecting the University motivating, and described their rationale for protecting the University with terms like “loyalty” and “pride.” In addition, they perceived that by offering Duo as a service, the University was looking out for their safety.

Social norms were important to people. People felt that they would be more motivated to adopt the behavior if they knew others were doing it. Many participants had no sense of what other people in their office were doing. Except for people whose express job it is to monitor information security, University of Minnesota employees do not tend to talk about their practices.

## Limitations and Future Research

The purpose of this study was exploratory, seeking only to get initial understanding of attitudes, social norms and behaviors, and the effects of persuasive messaging tactics. The focus groups were limited in number, and the number of participants was small. Therefore, the biggest limitation is that the data is not generalizable across the entire University of Minnesota population.

In addition, because the pool of participants was small and their availability limited, they were grouped by convenience, rather than by other more meaningful variables such as their experience with safe computing, their role at the University, or even their demographics. While there was good participation by all focus group members, future focus groups may be even more fruitful with homogenous groups of people based on their knowledge and experience with information security.

Another limitation of focus group data is that participants are asked to self-report on their behaviors, opinions, and beliefs. Self-reported data may be inconsistent with actual behavior or beliefs. Potential reasons could include misremembering or overstating (or understating) what one truly does or believes in order to fit in with the other members of the focus group.

The second part of these focus groups asked for reactions to two different printed flyer prototypes promoting safe computing behaviors. It is recommended that this exercise be revised and retested. In order to convey different tones, the prototypes shown had starkly different designs, graphic elements, and layout. Participants found it difficult to separate the design and layout of the documents from the content and tone. Participants had strong opinions about the imagery, colors, and text layout. While the researcher coached participants to avoid such critique, they were unable to separate the content from the design. To avoid this extraneous

discussion, future research should use the same color, layout and amount of content for both examples.

Also, recommended for future (generalizable) research, is an A/B test. The practice would involve dividing a single audience into two randomized segments. One segment would receive the fear-based message, and the other the rational, confidence building message. One could measure if the of messaging was persuasive by email open rates, link click rates, and in some cases, the download of the technology.

Finally, since information systems alone cannot protect people from cybercrime, and personal safe computing behavior is required, promoting a sense of personal responsibility is of particular interest for communicators. Understanding the reasons why people adopt an attitude of personal responsibility is a promising topic for future study.

## Recommendations for Communicators

Appeal to the resigned. The most common attitude expressed was that of resignation. One tactic that could be used to attract employees who are resigned to the inevitability of victimhood is to communicate the efficacy of adopting behaviors in order to engender a sense of hope.

Convey that safe computing is a social norm. Because safe computing is not a topic that is often discussed at the water cooler, communicating about it as a social norm is even more important. Therefore, it is recommended to prominently show statistics relating to adoption of safe computing behaviors. For example, it may be useful for University of Minnesota employees to know that 97 percent of employees in the Office of Information Technology have opted into Duo Protection for Direct Deposit.

Use storytelling. Several focus group members thought that hearing stories about real University employees would be most compelling to them. They want to know that real people who are just like them have lost their paychecks. For example, they would want to know that someone who used the same password for their University account and their LinkedIn account had their University email account hacked due to a security breach at LinkedIn.

Alternate appeals between fear-based and those that rational, confidence-building. Even though the majority of focus groups members believed that the fear-based messaging would be more effective in motivating action, there was positive response to the rational confidence-building messaging. Beyond building a sense of confidence, the rational messaging could be important to building trust between the sender and receiver and might contribute to improving the sender's reputation. In addition, there were a few who strongly preferred the positive messaging. It would be useful to leverage both tactics to be more inclusive of all audiences.

Alternate appeals between the selfish and the altruistic. Focus group participants felt that the altruistic messages were appealing. Several focus group members in different focus group discussions brought up the University's "Do it for the herd" campaign to encourage employees to get flu shots. Perhaps if alternated with self-interested messaging, the targeted safe computing behavior could have greater reach, or at least the function of reinforcing the behavior.

# References

(2016, July). Following the Links from Russian Hackers to the U.S. Election. New York Times, Retrieved from https://www.nytimes.com/interactive/2016/07/27/us/politics/trail-of-dnc-emails-russia-hacking.html)

A., & Cope, E. M. (1877). The rhetoric. Cambridge: Univ. Press.

Ajzen, Icek (1991). "The theory of planned behavior". Organizational Behavior and Human Decision Processes. 50 (2): 179–211

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Upper Saddle River, NJ: Prentice-Hall.

Anderson, C & Agarwal, R (2010). "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions". Management Information Systems Research Center. 34(3) 613-643.

Boss, S, Galetta, D, Lowry, P, Moody, G. & Polak P (2015). "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and fear that Motivate Protective Security Behaviors". Management Information Systems Research Center. 39(4) 837-864.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. European Journal of Information Systems,18(2), 151-164. doi:10.1057/ejis.2009.8

Brandom, Russell. (2017, May) The Google Docs spam attacks played off Google's most fundamental weakness: The dangers of an unwalled garden. The Verge. https://www.theverge.com/2017/5/4/15544608/google-docs-spam-phishing-email-hack-secure-account.

Chadwick, A. E. (2014). Toward a Theory of Persuasive Hope: Effects of Cognitive Appraisals, Hope Appeals, and Hope in the Context of Climate Change. Health Communication, 30(6), 598-611. doi:10.1080/10410236.2014.916777

Cyber Incident. (n.d.). Retrieved June 3, 2017, from https://www.ready.gov/cyber-incident

Dadisho, Edward. (2005). Identity Theft and Police Response: The Problem. The Police Chief.

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. Computers in Human Behavior,68, 359-367. doi:10.1016/j.chb.2016.11.044

Dow, B. J. (2017). Taking Trump Seriously: Persona and Presidential Politics in 2016. Womens Studies in Communication,40(2), 136-139. doi:10.1080/07491409.2017.1302258

Ernst and Young (2008) Fighting to close the gap. Van Kessel, Paul.

Finfgeld, D. L., Wongvatunyu, S., Conn, V. S., Grando, V. T., & Russell, C. L. (2003). Health Belief Model and Reversal Theory: a comparative analysis. Journal of Advanced Nursing,43(3), 288-297. doi:10.1046/j.1365-2648.2003.02712.x

Fitzduff, M. (2017). Why irrational politics appeals: understanding the allure of Trump. Santa Barbara, CA: Praeger, an imprint of ABC-CLIO, LLC.

G. R., & Berlo, D. K. (1960). The Process of Communication. College Composition and Communication,11(4), 250. doi:10.2307/355181

Herath, T., & Rao, H. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems,47(2), 154-165. doi:10.1016/j.dss.2009.02.005

Holbrook, M. B. (1978). "Beyond Attitude Structure: Toward the Informational Determinants of Attitude". Journal of Marketing Research, 15(4), 545. doi:10.2307/3150624

Johnston, A. & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. Management Information Systems Research Center. 34(3) 549-566.

Katz, D. (1960). The Functional Approach to the Study of Attitudes. Public Opinion Quarterly,24(2, Special Issue: Attitude Change), 163. doi:10.1086/266945

Larose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. Communications of the ACM, 51(3), 71-76. doi:10.1145/1325555.1325569

Lawson, S. T., Yeo, S. K., Yu, H., & Greene, E. (2016). The cyber-doom effect: The impact of fear appeals in the US cyber security debate. 2016 8th International Conference on Cyber Conflict (CyCon). doi:10.1109/cycon.2016.7529427

Leach, J. (2003). Improving user security behaviour. Computers & Security,22(8), 685-692. doi:10.1016/s0167-4048(03)00007-5

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. Behaviour & Information Technology,27(5), 445-454. doi:10.1080/01449290600879344

Lee, Matthew (2017, May) Miller, Microsoft Did Something Unexpected To Protect Windows Users From WannaCrypt Ransomware. Forbes. Retrieved from https://www.forbes.com/sites/leemathews/2017/05/13/microsoft-update-wannacrypt-ransomware/#62d73c3e77d7

Lee, Y., & Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. Communications of the ACM,48(8), 72. doi:10.1145/1076211.1076243

Lim, W. M., Teh, P., & Ahmed, P. K. (2014). Message sequencing of rational and emotional appeals: A study on consumer brand and product attitudes. 2014 IEEE International Conference on Industrial Engineering and Engineering Management. doi:10.1109/ieem.2014.7058863

Lipton, E, Sanger, D & Shane S. (2016, December). The Perfect Weapon: How Russian Cyberpower Invaded the U.S. New York Times, Retrieved from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology,19(5), 469-479. doi:10.1016/0022-1031(83)90023-9

Morgan, S. (2016, January 17). Cyber Crime Costs Projected To Reach $2 Trillion by 2019. Retrieved June 03, 2017, from https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/

Ng, B., Kankanhalli, A., & Xu, Y. (. (2009). Studying Users Computer Security Behavior: A Health Belief Perspective. Decision Support Systems. 46(4), 815-825. doi:10.1016/j.dss.2008.11.010

Öğütçü, G., Testik, Ö M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. Computers & Security,56, 83-93. doi:10.1016/j.cose.2015.10.002

Ovelgönne, M., Dumitras, T., Prakash, B. A., Subrahmanian, V. S., & Wang, B. (2017). Understanding the Relationship between Human Behavior and Susceptibility to Cyber-attacks. ACM Transactions on Intelligent Systems and Technology,8(4), 1-25. doi:10.1145/2890509

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. Computers & Security, 31(4), 597-611. doi:10.1016/j.cose.2011.12.010

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. The Journal of Psychology,91(1), 93-114. doi:10.1080/00223980.1975.9915803

Rosenstock I.M. (1974a) Historical origins of the Health Belief Model. Health Education Monographs 2, 328 – 335.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' Adherence to Information Security Policies: An Empirical Study. New Approaches for Security, Privacy and Trust in Complex Environments IFIP International Federation for Information Processing, 133-144. doi:10.1007/978-0-387-72367-9_12

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & Security, 24(2), 124-133. doi:10.1016/j.cose.2004.07.001

Steff, R. (2017). The audacity of Trump: How he won and what we missed. New Zealand International Review, 42(2), 2–5.

Vance, A., Eargle, D., Ouimet, K., & Straub, D. (2013). Enhancing Password Security through Interactive Fear Appeals: A Web-Based Field Experiment. 2013 46th Hawaii International Conference on System Sciences. doi:10.1109/hicss.2013.196

Wimmer, R. D. (2010). Mass media research. Belmont, CA: Wadsworth.Wood, W. (2000). Attitude Change: Persuasion and Social Influence. Annual Review of Psychology,51(1), 539-570. doi:10.1146/annurev.psych.51.1.539

Zhang, H., Sun, J., Liu, F., & Knight, J. G. (2014). Be rational or be emotional: advertising appeals, service types and consumer responses. European Journal of Marketing,48(11/12), 2105-2126. doi:10.1108/ejm-10-2012-0613

# Appendices

## Appendix A – Consent Form

**Consent Form**

You are invited to be in a research focus group about message that motivate the adoption of safe computing behaviors by staff at the University of Minnesota. Please read this form and contact the researcher with any questions you may have before beginning this study.

*This study is being conducted by:*

Kelline Greaves, Strategic Communication Master's Candidate, School of Journalism and Mass Communication, University of Minnesota, kellie@umn.edu
You can also contact the academic advisor, Dr. Stacey Kanihan at skanihan@umn.edu

If you have any questions or concerns regarding this study and would like to talk to someone other than the researcher(s), you are encouraged to contact the Research Subjects' Advocate Line, D528 Mayo, 420 Delaware St. Southeast, Minneapolis, Minnesota 55455; (612) 625-1650.

*Procedure:*
If you agree to participate in this study, you will be asked to attend a focus group about the messages about safe computing behaviors at the University of Minnesota. You will also be asked to provide some demographic information. The focus group will last approximately 60 minutes.

*Risks and benefits of being in this study:*
There is no particular risk associated with this study.

*Confidentiality:*
The information you provide in this survey will be kept private. Only the researcher will have access to the records. Data included in the final report will not include any information that would make it possible to identify a study subject.

*Voluntary nature of the study:*
Participation in this study is voluntary. Your decision not to participate will not impact your standing with the University of Minnesota. If you decide to participate, you are free to not answer any question or to withdraw from the study at any time.

Please sign to acknowledge your consent to participate in this focus group

_____ Date _____

## Appendix B – Focus Group Instructions

### Script for Safe Computing Focus Group

Introductions (10 minutes)
You just signed our agreement form for participants. Did you have any questions about anything on the form?

1. You can leave at any time. If you want to take a break for any reason, you may leave and come back.
2. There are no right or wrong answers today—I'm interested in finding out your thoughts and opinions, and I value your perspective.
3. I am taking audio and video recordings, but your participation is confidential and any notes or reports produced from the session won't reveal your identity.

Today, I want to learn about your what you know and think about safe computing behaviors.

- Before we start, let me suggest some things to make our discussion more productive.
- Please speak up so all of us can hear you, and speak one-at-a-time so we can give you our full attention.
- Please feel free to share your perspective, even when it differs from what others have said—especially when it differs from what others have said.
- I'm just as interested in negative comments as positive comments; at times, the negative comments are the most helpful.

Introductions
Let's begin with a quick round of introductions…

Let's go around and share our names, title, department or unit where we work, and If I could put you on a plane to anywhere in the world after this discussion, where would it be and why?

**Appendix C – Fear-Based Flyer**

Are you doing all you can to protect your SSN & paycheck?

**YOU ARE A TARGET FOR IDENTITY THEFT**

**People just like you fall prey to sophisticated cyber thieves every day**

Phishing emails are like wolves in sheep's clothing. They pretend to be from friends, colleagues, or organizations you know in order to trick you into giving up your password or other personal information.

Criminals then use your password to gain access to information your password is meant to protect, like your Social Security Number and bank account.

**Stop criminals from stealing your Social Security Number or paycheck**

Duo Protection for W-2 and Direct Deposit is a free service available to University employees that helps keep criminals out of your accounts. It works by verifying your identity with **two factors**: something you *know* (your password) + something you *have* (your smart device or other phone number). After you opt in, thieves would need your password AND your phone. Only you have both.

**Take 10 minutes to Opt into Duo Protection today: z.umn.edu/duoprotection**

Keep your accounts more secure. Set aside 10 minutes with your computer and your smart phone or tablet (or other phone number) and follow our step-by-step instructions at z.umn.edu/duoprotection. If you need help or have questions, call us at Technology Help at 612-301-4357 (1-HELP)

For disability accommodations, call 612-626-1333 or email ds@umn.edu.
Call 612-625-1666 for document conversion.

The University of Minnesota is an equal opportunity educator and employer.

**Appendix D – Rational, Confidence-Building Flyer**

# **You can** help protect your identity from theft

Phishing emails are one of the tools criminals use to steal your identity or account information. They have become very sophisticated and look like authentic emails from people or organizations you know. If your password is stolen, access to your accounts can be just a few clicks away.

While being vigilant helps, the University of Minnesota offers a free service so you can take action to help ensure that you **and only you** can access your W-2 and Direct Deposit information: Duo Protection for W-2 & Direct Deposit.

**Duo & you can make a difference**

You sign up, then Duo Protection will require two "factors" to access your personal W-2 and Direct Deposit information: your password + a verification from your smart device or phone. Only you have both your password and phone, so only you can access your accounts.

Sign up today at **z.umn.edu/duoprotection**. It'll take just ten minutes with your computer and your device or phone. Step-by-step instructions will guide you through the process and you'll feel great knowing you've added another defense in front of your SSN and bank account information.

For disability accommodations, call 612-626-1333 or email ds@umn.edu. Call 612-625-1666 for document conversion.

The University of Minnesota is an equal opportunity educator and employer.

## Appendix E – Focus Group Notes

### Focus Group 1

#### *Participants*

| Focus group 1 member identifier | Age range | Gender | Education | Marital status? | Ethnicity | Familiar with term "safe computing?" | Have you ever received a phishing email | Has your password, credit card number, bank account number, or social security number ever been stolen? | What is your level of concern re: cyber crime | Probable victim of cybercrime? |
|---|---|---|---|---|---|---|---|---|---|---|
| F1-1 | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported |
| F1-2 | 35 - 44 | Female | Professional degree | Divorced | White | Yes | Yes | Yes | Slightly concerned | Somewhat probable |
| F1-3 | 45 - 54 | Female | Professional degree | Married | White | Yes | Yes | No | Slightly concerned | Not probable |
| F1-4 | 55 - 64 | Female | 4-year degree | Widowed | White | Yes | Yes | Yes | Moderately concerned | Somewhat probable |
| F1-5 | 35 - 44 | Male | Professional degree | Married | White | Yes | Yes | Yes | Slightly concerned | Somewhat probable |
| F1-6 | 55 - 64 | Female | Some college | Married | White | Yes | Yes | Yes | Extremely concerned | Somewhat probable |

#### *Notes*

**I'd like to hear about your experience with and perceptions about safe computing. What are some of the thoughts that come to mind when you hear those words.**

F1-5 - Scams

F1-6 - Be careful

F1-3 - Habits

F1-2 - Exposure

F1-1 - People will click on anything

F1-4 - Backups

**Thinking about your own behavior, what are some of the thoughts and feelings you have about your own computing behavior?**

F1-4 - Hope for the best

F1-6 - Strong passwords

F1-4 - Caution

F1-5 - I accept. I do the basics, I do backups. I do passwords, but like, I've accepted. My identity has been stolen and terrible things will happen. That's just a thing you live with.

F1-3 - I think it's really about how can I get things back up and running and restore things as soon as possible should it happen so I won't be out of work for very long.

F1-1 - Temptation I would say, because you know it's really tempting when you're doing other things to just log onto your bank account from a coffee shop. Checking or whatever it happens to be. Even though I have the Cisco client on my computer, so I can get a secure connection to the U, it doesn't always work from some coffee shops for some reason, and then you're tempted just to go do your stuff anyways. That's why I said habits.

**Do you know what your friends and colleagues do for safe computing?**

F1-3 - My colleagues frighten me. I mean especially outside of the technology realm. In this day and age, there is no reason to keep anything you care about only on your computer, you know a lot of people do, including previous studies and when you lose that computer, it's just gone. You know it's funny. I think a lot about this from the Hillary Clinton email. I mean that was, when it came down to it, that was people not knowing what they were doing. So that frightens me--what people don't know about security on a basic level.

F1-5 - Even my friends in IT don't use password managers or basic stuff.

F1-4 - I think we talk about it a lot, but I'm not sure that anyone has come up with something that they're really comfortable with. We all moan. It's like you were saying, it's an inevitability, it happens and we all move forward.

F1-6- I think our department uses S-drive. (about saving files to a shared drive/rather than storing it on one's own computer)

**Where do you think people/you learn about safe computing...how do you recognize scams or learn about them?**

F1-6 - Well on an email, you look to see where it's from. It's kind of a tip off.

F1-1 - If you look at your email and you see long headers, you can get a sense if it's legitimate, even if it had a friend's name on it, if you don't do long headers, it's usually...If there is a scam

in CBS, Mike Waltonen sends out emails on a pretty regular basis letting people know if there is something out there. That's where my colleagues get their information.

F1-5 - With the recent one with Google drive it was on the tech people slack right away. But, of course if people read their email linearly, they've already gotten to the scam email. That's a tough problem to solve.

F1-4 - I think I learn from things online. Top ten ways to avoid this or that. Emails that come from the U, from my college, mistakes.

F1-1 - I was at a conference and I was talking to people about their agents, and their agents won't even accept anything with an attachment. If you want to send anything to them, it has to be in the body of an email. I don't know where that is coming from, but it's the zeitgeist. People are talking about it. It just shows that people know that clicking on something that comes in an email can be dangerous.

F1-5 - There are general blanket, and then there are targeted where if a group really wants to get into someone's email. We get post-mortems, where people are compromising these other accounts, get a password from this account and get this cell service provider to access with a two-factor code. If they really want to get in...You can see that with political hacks as well, with the spear phishing. That's the point where I say, if someone really wants to read my email, they can probably read my email, there's not much I can do about that.

F1-2 - So I don't read, "Hacker" whatever. I really rely on if U of M IT is going to keep sending me reminders, I will pay attention to that. When I saw the Duo factor thing. I didn't know what that was, and didn't know that it was a best practice. (pointing to F1-5) you said password manager, that makes me think, "Is that a good thing or a bad thing or an okay thing?" I don't know. And the words "Safe Computing" are so fundamentally sort of boring to me that I'm not going to sign up for a service that is going to keep me up to date about that.

**What would be a term that would be appealing? Do you feel like people understand the consequences of having their identity stolen?**

F1-1 - I don't think that people realize the consequences of getting into a car. It's one of those things that you have to do on a daily basis so you sublimate the risk factors.

**So, you would put on a seat belt, right?**

F1-1- It took until we made a habit of it.

F1-5 - I think in the IT world we're good at saying use Duo, but we're not good at educating why and how to translate that to your personal Twitter account. We tell you about Duo, but we don't tell you about 2-factor and why it's important.

F1-4 - Do we ever get to the point of testing or tricking people? My daughter sends out fake emails once a month and if you click on it, you get a little alarm.

F1-1 - It seems like the same sort of scenario for the health benefit where we get $400 per year for getting these health points, there's a gaming mentality and a reward mentality. You don't look after your long-term health necessarily unless somebody incentivizes you.

F1-4 - Or if you have a scare. If you get hacked, you're more vigilant.

F1-1 - But then the question is with those, after you get your points, then do you stop caring about that?

**Is it authentic participation or is it jumping through the hoop?**

F1-1 - It's the same problem. The risk is so far out there, that it's hard to pay attention to it. If the behaviors are cumulative and they add up to good practices, maybe you end up with more secure

**Have you had conversations with people in your offices about identity theft? Is that front-of-mind enough?**

F1-2 - I most often hear about passwords and how frustrating that is. So, I'm often telling people my awesome password formula because I don't use a password manager. That's the only conversation I have with people about this, unless something happens to them.

**After the recent Google Drive Scam, did you have conversations about phishing?**

F1-5 - We had conversations about response...is it better to put something out right away? I had a couple of cases of identity theft...once your social security number is sitting on a spreadsheet.

F1-6 - We had some light conversations, but nothing that got in depth. This is so stupid. What a waste of money.

F1-4 - We had casual conversations, nothing really in depth.

**Do you know people who fell for it, or had to reset their passwords because of the incident?**

F1-2 No comment.

**Wolf flyer - take a few minutes to read it, write down comments, thoughts you have as you review it. What are key takeaways?**

F1-6 - I'd make the wolf's face a little bit bigger. I didn't realize it was a wolf at first.

F1-5 - Two sets of eyes were disturbing

F1-6 - The words "set aside" turned me off. Seriously? It should just be click here!

**Elaborate on that.**

F1-6 - Setting aside 10 minutes, where am I going to set aside 10 minutes. That might happen next week, or two weeks from now. It took away all the urgency.

**I see, so you don't have ten minutes?**

F1-6 - Setting aside the 10 minutes is the problem.

F1-5 – So, blocking out time, not just doing it.

F1-6 - If you take the "set aside" out and just put "click here" we'll walk you through it.

**We got feedback, you can't just do it in a meeting. It's not the easiest process, you actually need 10 minutes with your computer and phone. It's good to know that it undermines the urgency.**

F1-2 - I thought the imagery was clever and I like the subheads. The rest of it was clearly written, but wordy. On a flyer, it may be too much information. If it is sending me to your website, that's where that should go.

F1-5 - If it is just about SSN and paycheck, I would flip the two. "You're a target for identity theft" I accept that, right? The paycheck is more of a threat.

F1-2 - It felt like the most important part was buried in the last sentence in the second section. Opt in is the main thing that would convince me of the efficacy of duo protection.

F1-3 - I think you need to demystify Duo protection as well. In my crowd, they would say duo protection, I don't know what that is, I'm not going to deal with it. They completely tune out as soon as they don't know what it is.

**So, the wordy part, kind of gets to what two factor is...**

F1-3 - It explains what two factor is. I thought really well. But, it doesn't say why do I need two factor.

F1-5 - Rather than the brand of Duo.

F1-6 - Two-step verification?

**What would you recommend?**

F1-3 - People actually do care about security, but it freaks them out too. Basically, what works where I work is that we just have to walk them through it.

**So, any kind of email or flyer, doesn't do it. They really need face to face.**

F1-3 - Yep. They want their hand held through it.

F1-1 - "You are a target" is like a truism. Also, I don't care about my SSN as I do about my paycheck. When you say, "Are you doing everything you can to protect your paycheck?" I don't really know what you're asking me. It's like, am I going to get fired? Then I would say people like you fall prey to sophisticated...then I would say stop criminals from stealing your paycheck. And then everything else can get tucked away as far as I'm concerned. Take ten minutes, or

maybe it you can't do it now, you can schedule a couple of reminder emails. The headline gets lost on this flyer visually. There is some confusion about the metaphor. The wolf in sheep's clothing goes well with the identity theft, but maybe not the rest of it. Maybe phishing is a more apt metaphor?

**Does this message seem threatening to you? Does it raise urgency at all?**

F1-2 - It doesn't. While I get the idea of talking to people's bottom line, and that is the way of motivating them. I just have such confidence that if my paycheck stolen, there would be some recourse for getting that money back. But if what happened to Hillary happened to me, and my emails were made public, I would be worried about my reputation. Now you're probably wondering what I keep in my emails, but. Like you could be embarrassed and you can't get your reputation back.

F1-5 - You work for a public institution, all of your UMN emails are public.

F1-2 - Thanks for reminding me of that.

F1-2 -My emails represent more of threat. They are something that is less easily reclaimed.

F1-5 - Opt into" rather than "activate" Duo Protection - I associate it with something that is not urgent, "opt into our emails"

F1-3 - The best way that we've had improvement is that we're moving our data management to Box. And you need Duo for box. People need a purpose for it that has to do directly with their work. No one has been freaked out about getting Duo in order to access Box. Then we couple it with that.

F1-2 - It's voluntary for us, but thinking about new employees, could it be mandatory?

**Did anyone else perceive a threat?**

F1-6 - I'm pretty easy to threaten, so actually for me, it did.

F1-2 - It made me question, I already signed up for this, didn't I?

**Does it seem like appropriate messaging coming from the University?**

F1-5 - I don't think it's out of the norm.

**What are some of the key takeaways you have from the blue one?**

F1-6 - I didn't want to read it.

F1-5 - She's way too happy. The laptop is ten years old.

F1-1 - Image is not great. It might need to be an illustration. Needs a hood. You're not getting the problem. The headline isn't strong enough.

F1-5 - The text was too hard to read.

**Design aside, the text that you did read...what are your takeaways?**

F1-2 - It's too wordy. I would have two or three key points and drive everybody to the website. Where people have more time to take it and read a little bit more.

**So, if the content were on the website, what do you pull from that?**

F1-2 It would be good to describe it in bullet points, maybe.

F1-5 - Visually maybe?

F1-3 - I don't want to read all of this stuff. Just tell me what to do, and I'll evaluate the steps to see how hard it is. Is it hard? No. Go here, do this, done.

F1-6 - More like a road sign. You can see it when you're traveling.

F1-1 - I think the tone is much different from the other one. I think it's geared toward someone who is not in this room. If someone doesn't understand the problem at all. It feels like, I might

send this to my mom. If it went out to most of the people in this room, it's not gonna...If you already have some familiarity with. It's a little condescending.

F1-2 - I had that reaction too. It diluted the call to action here. So that's the only reason, for my great feelings? Because I'm certainly not going to read these two paragraphs about it.

F1-5 - It feels like it's over-promising because it's not 100% effective.

F1-3 - The tone didn't bother me at all and I didn't notice the picture.

F1-2 - Corporate stock photography is just not motivating.

**Looking at the two pieces comparatively, are they motivating you to take action?**

F1-5 - The wolf one is much more. The blue one is like Smokey the Bear.

F1-3 - Although Smokey is getting edgier.

F1-4 - I'm probably 50/50 either way.

F1-1 - I'm thinking about when I got the email and signed up for it, why. To me. It's an insurance policy. It was a bit of a pain to do it.

F1-6 - Could you call it insurance? Give it a tweak?

F1-1 - With a few tweaks, the first one creates a sense of urgency, or anxiety in general. Your paycheck is very important it's urgent. The other thing gives you a sense of agency. There is something you can do. You don't feel scared then. Those things have to follow close without a lot of distractions.

**Does anyone have ideas about how to motivate safe computing behaviors?**

F1-4 - Staff meetings - talk about it. Work related first, and having ways to protect. It's a small staff.

F1-2 - Doing it all at the same time. Like fluoride rinse days.

F1-1 - The university doesn't want to mandate this, faculty may not do it, but if their lab employees do it, they are advocates, and they become ...it works better if you set up the expectation. If my boss said that we'd like everyone to do it, if you have a good reason, talk to me. But I would just do it.

**Do you look at anything on paper?**

F1-1 No. Unless it's employee benefits and compensation.

F1-2 - I recycle.

F1-3 -If it were part of your benefits. - this is part of your health.

F1-1 - I don't look at my paycheck often. If there were a pop up, I might pay attention. Even if there were something on your pay report. Short and compelling.

**Do you look at posters?**

F1-6 Least likely to look at posters.

F1-1 - Need a certain number of impressions, posters might be one or two of the impressions so they finally see them. You would have to talk about a campaign.

F1-6 - Email is easiest because you can click the link.

F1-1 – I saw it when it came up on MyU.

**Have you noticed our safe computing campaign - once a month a new topic?**

F1-1 - I don't click on it. It looks like something that I have done before through HR, and I got no value out of it.

**Focus Group 2**

***Participants***

| Focus group 2 member identifier | Age range | Gender | Education | Marital status? | Ethnicity | Familiar with term "safe computing?" | Have you ever received a phishing email | Has your password, credit card number, bank account number, or social security number ever been stolen? | What is your level of concern re: cyber crime | Probable victim of cybercrime? |
|---|---|---|---|---|---|---|---|---|---|---|
| F2-1 | 35 - 44 | Female | 4-year degree | Married | White | Yes | Yes | No | Extremely concerned | Somewhat probable |
| F2-2 | 25 - 34 | Female | 4-year degree | Married | White | Yes | Yes | Yes | Moderately concerned | Neutral |
| F2-3 | 25 - 34 | Female | Professional degree | Married | White | Yes | Yes | Yes | Slightly concerned | Neutral |
| F2-4 | 55 - 64 | Male | 45 - 54 | Male | 4-year degree | Married | White | Yes | Yes | No |
| F2-5 | 25 - 34 | Female | 4-year degree | Never married | White | Yes | Yes | Yes | Extremely concerned | Neutral |
| F2-6 | 45 - 54 | Male | 4-year degree | Never married | White | Yes | Yes | Yes | Moderately concerned | Very probable |

## Participants

Eighteen University of Minnesota employees participated in three focus groups (six participants per focus group). Thirteen of the participants completed the survey. The focus groups were formed based only on participant availability, rather than on demographic data or experience with safe computing or cybercrime.

### *Notes*

**Experience and perceptions about safe computing. Thoughts or words that come to mind when you hear the term "Safe Computing"**

F2-1 - Encryption

F2-4 - Protecting yourself from things like phishing...malevolent links on web pages

F2-6 - Virus protection

F2-2 - Trying to keep ahead of the people who are doing the phishing

F2-5 - Antispyware

F2-3 - Keeping things patched

**What are some of the feeling you have around safe computing**

F2-1 - Embarrassment when you don't do it right.

F2-6 - Am I doing enough? Am I safe enough?

F2-5 - Right. Anxiety about if I am missing something. Is there something I should have configured?

F2-2 - I am sure I am missing something. There are Duo...Duo entry, and I don't know the right words. So those are things that I know I could do, but for whatever reason, but for some reason, I haven't yet. It makes me feel like I could do a little more about that.

F2-4 - I feel a great deal of concern globally and nationally about the lack of concern for safe computing and how willing people are to give away their private information and what the consequences of what that might be over time.

F2-3 - I feel real nervous about old people who don't understand the internet very well. They aren't as concerned about clicking on links and downloading things and like "winning a prize."

**Are they people in your life, or just a general concern?**

F2-3 - Just a general concern.

F2-1 - I definitely have grandparents who have all been scammed repeatedly through not safely computing. There is definitely a fear for them more than anything else.

**Why do you think you know about safe computing, and they don't?**

F2-1 - Because I was really young when I started using a computer and they were in their late fifties. So, I think it just is intuitive to me.

F2-4 - We hear about it more working on computers all day every day. Working at the U too, it's in your face. My dad just got one, so it's not at the forefront at all.

F2-3 - ...and it's kind of like if old people are equating email to US mail, usually, there are some scams through US mail, but they don't take over your life very quickly. And say if you think a computer is a glorified typewriter or the internet is a glorified telephone network system, or something like that, it doesn't translate quite correctly to reality.

**What are some of the safe computing practices or tools that you use, or that your colleagues or friends use?**

F2-4 - I think one of the most important things is just to be always aware and vigilant that there are people who want to do nefarious things and you just need to be not gullible about things.

**Do you know if people on your team are aware or vigilant or use safe passwords?**

F2-4 - Yeah, definitely the people on my team pick out things. We get emails fairly frequently and some of them are very good and people look at it right away and think that looks like phishing and then we start to get emails that come in, "I clicked on this and blah, blah, blah happened." You know, if you were more skeptical about stuff, that you'd be much safer.

F2-5 – Yeah, it seems like a simple thing, but just recently when the U of M had that...I was texting my boss who is now retired saying don't click on that.

F2-4 - Yeah. That was one that looked very real. I think we're talking about the same thing...the Google Doc sharing?

F2-5 - Yeah.

F2-1 - It was much larger than just at the U.

F2-6 - I saw it happen over Twitter.

F2-4 - And that is the one I was thinking about pretty much in particular. Everybody in my office all at once said, I just got this weird thing. Very shortly after that we started getting things like "Oh I clicked on this...and what do I do now?

F2-3 - One of my coworkers who is a little bit older asks a lot, like [name] did you get this email? It looks weird, should I open it. And I say, delete it, Mary.

F2-5 - At least she's asking.

F2-3 - I know! I try to reframe, like she's interested, she wants to do the right thing.

F2-5 - There's something going on...I better ask about this.

F2-3 - But her safe computing technique is asking me.

F2-5 - If I send a Google form to people, I historically have to order their computers and find out what they need, and there were quite a few people that would call to make sure that I actually sent that, and they should actually click through. Because they had clicked something wrong in the past and they were afraid then to repeat that mistake.

F2-3 - I went to a safe computing workshop recently and after that a coworker was working from home and G-chatted me like hey, can you log into my computer for me, and I was like, "I'm gonna call you!" and I felt very proud of myself.

**What motivated you to go the safe computing workshop?**

F2-3 Um...strong wording from central administration to please attend this workshop and then I was also curious, and it was well done.

**How about the rest of you? About what your colleagues know, or if you ever talk about safe computing?**

F2-2 - My coworker who is about my age was the one who sent me an internet link to five steps you should know about internet safety and they were things like use VPN, and I think she did most of them and I didn't do any of them. I think she took action on at least a couple of them.

F2-4 - I think I do all of the things that we're mandated to do, or that I'm told to do through the U in terms of the Duo two-factor authentication, the forced changing of your Internet x.500 password, but then I probably don't do enough of it in my personal life as far as all the other passwords. It's one thing keeping them sort of similar so that you can remember them but then when they're telling you to change all your other passwords all the time, I could spend all my day trying to keep track of all the passwords.

F2-6 - Yeah, it's a huge demand. I feel frustrated that vendors don't supply things that are more safe out of the box, you know things like your home router, I keep hearing things more and more about how the IoT is pretty much unprotected. Whatever device that you have online can probably be hacked and used maybe not to affect your life negatively, but bits of computing

power hijacked or its camera hijacked or something that can affect other people negatively, I think most often it seems like it should just come safely configured out of the box.

**When you hear about new safe computing kind of standards or behaviors, do you assess, like do you think this will actually help me, I think it will actually work. Turns to F2-2, I'll call on you because you've seen a list of things that you ought to do.**

F2-2 - I may be nervous that there is some technical piece that I don't know, and maybe that's why I'm not starting to...they can give me steps, but I can look at that and feel like I'm not quite sure I know how to do that and then don't take action to find someone who can help me with it.

F2-1 – Sometimes, there is cost that goes along...like with a VPN. I'm kind of like you, when I trust the U to keep us safe here and when I'm at home, it's in my husband's wheelhouse to pay attention to that stuff and research that stuff and he is on it. But there is a cost for VPN, but he pays a certain amount every year to make sure we're safe at home. Not everyone has the know-how to do that or the money to pay for it, which is…

F2-6 – Sometimes, things don't work properly. Then it's like why can't I print now? Or why or whatever and that is a big pain.

F2-1 – So, if it came out of the box safer, then it would be encompassed in the charge.

F2-5 - I tend to feel a little skeptical that things will be more protective than me just being smart about what I'm browsing what websites I'm going to, that kind of thing. I'm careful about

downloading things, and I think that those extra steps are meant to make you feel safer, but don't necessarily protect you.

F2-1 - I think it's more in the forefront with that net neutrality issue and with the government and if they can just start selling our information it's a reason to look into more solutions.

**Are you able to pinpoint where you learn about safe computing? Is it talking with peers?**

F2-3 - 'Reply All" a podcast about the internet. They had an amazing couple of episodes about phishing. Things like that, and then extension IT does alright.

F2-5 - My office put together a video where they rapped, I believe. I actually never watched it because I was kind of turned off by the premise but it was about phishing. There was an episode of one of those addiction shows and someone was addicted to the internet and they were convinced that they were going to make all this money from an investment with a Kenyan king...you know those scams and I feel like that was one of the first times I heard about it...it was like over ten years ago. And it was like oh! That's how these things happen. People get so sucked in that they forget all of reality.

**When you are online, how confident or unconfident do you feel about your safety? When you are online shopping or working. How much anxiety or vigilance do you have around just being on your computer or being online.**

F2-1 - Not too much anxiety. You can fall down a rabbit hole of anxiety about almost everything in life, your kids or your safety but I don't try to feel too anxious. I've gone this many years

without anything happening to me, and then you just start to feel safe and maybe that isn't the best feeling in the end, but I definitely learned how to make my passwords stronger and it is helpful when websites give you, you know that little green bar to say whether it's stronger. You know I def. Think more about those things than I did even five years ago. But again, I've been this safe for this long, so I just kinda lose that anxiety too.

F2-2 - I would say I don't think about it a lot until I read something or get a newsletter from OIT or something. That makes me think about it. And then I think could I do this or that? But just in a general workday or reading Twitter on the bus, I don't worry about it too much. I feel like part of this is separate. And we'll see if this makes sense, in my brain, where I am almost resigned to the fact that amazon knows everything that I might want to buy and that type of online awareness...I'm fine with that. I understand that's happening. When I look at something over here, Facebook is showing me the ad I accept it. People are weirded out about it, but I accept that. But things where they are taking over my hard drive and I lose all 13k photos of my son and I have to pay bitcoin, and I don't know what that is. Like the stories and more extreme in the news, I don't really know what would happen if something like that were to ever happen. But I'm going to be skeptical enough not to click on that Gmail link probably.

F2-3 - I feel like there are two big buckets of vulnerability and one is your email and I feel like I'm savvy enough to not have to worry about that one too much, and the other is browsing on the internet and I also don't worry about that too much because I've also accepted that everyone already knows everything about me so they can market to me, but again it also comes down to,

make sure you don't download anything from the non-reputable site. And I feel like I just don't download a lot of stuff anymore.

**What about online banking or shopping?**

F2-3 - I trust my credit union and my credit card. Especially my credit card number has been stolen multiple times and I always get a phone call and am always off the hook. So that system has worked repeatedly well for me.

F2-6 - Same.

F2-3 - I'm lulled into a sense of security. How false that is, I don't care to consider. I don't do a ton of online shopping either, so it's doesn't present a huge concern to me.

F2-5 - I do a lot of online shopping but the only time I've had my credit card information compromised was when it was at Target and it was when they had that huge...so obviously, you're never safe. I'm not concerned as long as the store that I'm shopping at…

F2-4 - But again, that's an online system. So, you're not physically on the internet, but you're on the internet. You're trusting that someone else is doing it right.

F2-3 - Thanks, [F2-4]

F2-4 - Well, and lately there's been quite a bit about the credit card scam...the device that they can put on gas pumps and stuff like that so you don't even really notice but they're skimmers.

F2-4 - Skimmers, yeah. I feel really safe in the work environment, again. I get spam you know, but I get lucky because everything pretty much that I send that is personal is from a different email. I feel pretty safe on doing transactions but I don't do much online shopping. But, even if I am ordering something for travel I think a little bit about it. The one time my credit card got stolen it was at an internet coffee shop or whatever, ten or twelve years ago, so I think I learned not to do transactions from there. But you just don't know. Like you use wireless at hotels to make some other further reservation, is that more dangerous than like a secure thing. So, I'm just like hoping something doesn't happen. But I just figure too, if my number is up, then so be it. Like my neighbor across the alley just had his identity stolen and he didn't really know how and he's super bright and young, so I just figure, if your number's up.

F2-6 - and it's really hard to tell too, like you can't identify where that happened.

F2-2 - Exactly.

F2-6 - My wife has had the same thing too. Her credit card has been used a couple times to do things and her credit card company has been really good about contacting her about it. But it's like, "where did they get that?" You don't know if it's at a store or a skimmer at a gas pump or you know where it came from.

F2-3 - You know it's like, at some point, I might get into a car accident. I'm always going to drive as safely as I can, but it's not always within my control.

**How about identity theft. Do you worry about that?**

F2-6 - Yeah, my wife actually had her social security number stolen before we met. Someone had opened a cell phone account in her name and it almost made her not able to buy a house because she didn't find out about it until she went to get a loan and they said, said you are way in default on this cell phone account. And she's like "I don't have a cell phone." And it took a long time to get it straightened out and she probably wouldn't have been able to buy a house had her parents not intervened and helped her with that. It was a big deal. By the time I came along, she had it straightened out but it consumed a lot of her life to get that fixed.

**Does that affect...does identity theft...affect your behavior online?**

F2-5 - It scares me, but kind of like you were saying, if it happens, there are so many ways that it could happen that I don't know how to prevent it fully beyond what I already do just to be safe. I'm not going out of my way to protect against identity theft, but it's a concern.

F2-3 - I remember I had to use my SSN a lot more when I had student loans and stuff. It's like, I sure hope you're secure.

F2-1 - I was just thinking, when do I have to enter my social?

F2-5 - A lot of banks have you do that too.

F2-4 - It seems like their moving away from that.

F2-6 - Right. Back in the days of paper checks many vendors would require that you write your SSN on the check. I can't even imagine doing that now.

**Wolf in Sheep's Clothing**

**What are some of the thought you have about what it's trying to say to you? Is it compelling?**

F2-3 - I think the most compelling thing is "am I protecting my paycheck?" That's not something that I think is vulnerable, but based on the workshop that I went to, she described how...yep you could lose money and the U used to reimburse you, but they're not going to reimburse people anymore, and I was like, "Oh! That sounds bad." When it was made more real for me, in that way. Here's a direct consequence that happened to other people and it's going to be even worse. Seeing "paycheck" on here is like that is something I want to protect. Because we all know protecting our SSN is important but we don't think about the consequences of what does happen.

F2-5 - I would say that it would be more effective if it said, the U will not reimburse you if this happens.

F2-6- Mmm. Hmmm.

F2-5 - I see this and I say, Okay, but there are so many steps in place if something happens like there are things you can do. If it does happen to people like me, there are probably things that happen after the fact. I'm glad it has the word "sophisticated" because sometimes I read things like this, and I feel like they're condescending and I feel like I'm better than that. So that is helpful language to feel less… but it is a little fear-mongering. Without specifically talking about that kind of consequence.

**And being fear-mongery...does that put you off?**

F2-5 - A little bit, yeah. I kind of think that these types of things can be condescending and so I don't consider myself the audience for things like this. And when it is fear mongering, I tend to think this is too much. I especially think it isn't for me then.

F2-1 - I like that it isn't just saying you are a target, so be careful, but it offers solutions. And then it tells you how long it will take.

F2-5 - yeah. The 10-minutes thing is helpful.

F2-1 -You're not going to have to take an hour. Those are two pluses.

F2-6 - I'm a little skeptical when someone says it'll take ten minutes to do this, but I agree that it's helpful to have an idea that this is not going to take you half a day or something.

F2-1 - It isn't fill out this form, and send it here, and then you have to…

F2-4 - Right. Right. Right.

F2-6 - It's like one website.

F2-4 - Well, maybe there are questions and if you just rattle off the first thing that came into your head, it would take you 30 seconds or dig up the real information that is going to take you a lot longer.

F2-1 – Yeah, to get my benefits here, I had to dig up my marriage certificate.

F2-6 - I feel like things like this are important, but it does take extra convincing for me. Like I knew I should opt into the Duo thing. But I know that every time I do something like that it is a little more inconvenient. I mean everything works right now, but what if I opt in and I get locked out.

F2-5 - Why rock the boat?

F2-6 - Why rock the boat! Exactly! I did have a thing that I opted into Duo and I wanted to log into something, and I only set it up on my phone but then I didn't have my phone with me, and then it's like now I can't get at it anymore. So, I'm always a little skeptical of stuff like that

although I know it helps and it's important. But it's like you make it more complicated for yourself too. You make it more complicated for other people to hack you, but it makes your own life harder too.

**Does this communicate urgency? Everyone has their own equation. My boss tells me, or this is a real threat to me, or should do this because I feel guilty...when you read this, is there a compelling reason for you to take 10 minutes to go through what you think might be inconvenient.**

F2-3 - I think it would be more compelling if I knew how many people had money stolen from their paychecks or if I knew how many people had already opted into Duo protection because I would be part of a crowd that is doing the right thing. Instead of like continuing with the secret shame that I have. There is one thing that each year, I get a flu vaccination...like do it for the herd. I don't want to be that person who gets the flu and then spreads it to three other people.

F2-6 - That's interesting. I was just thinking about the do it for the herd thing and there is something to be said for that with safe computing. You are kind of doing it for the herd too because you know if someone on your network gets hacked, that can be your issue too. Or if someone at the desk next to you clicks on some phishing thing, that compromises the server you're both on, that's an issue too.

F2-3 - Another compelling thing from the workshop was that we as University employees our information unlocks a world of information and resources. Just thinking about what we have access to through the libraries, that stuff is so valuable. That to me was like, okay this stuff I have access to is really valuable and could be a target for more people than just all of my

personal information. So that..,tapping into you work at the U, if you're an engaged employee you probably care about the U to some extent, like this isn't just about you. But also like having a story about people losing their paychecks. There is a selfless and selfish reason for safe computing at the U.

F2-2 - I get the sense that it is somewhat urgent but not completely urgent. It seems urgent because there have been multiple emails urging you to do it. But I agree that maybe some stats on repercussions for not doing it, or how many people were negatively affected.

F2-5 - Or information about how long it takes a person to get their stuff figured out after their SSN is stolen.

F2-4 – Yeah, yeah, yeah!

F2-5 - 10 minutes will save you five 5 years.

F2-5 - I will say, if there were more statistics or specifics then it wouldn't feel as fear mongering to me. When it is very general, it feels like it's just trying to scare you and not actually giving you real information.

F2-3 - And the wolf in sheep's clothing imagery just does not land with me.

F2-4 - The other thing, with the whole numbers thing, I remember hearing way back when, when I was in high school when my family had to fill out financial forms (FAFSA) it took a long time, and I remember somebody saying, yeah but it if winds up getting you x amount in grants, that you made $2,000 an hour while you were filling it out. Something like this, if people's paychecks have actually been stolen. Say your paycheck was a thousand dollars, then it took you ten minutes, you're making 60 thousand dollars an hour by doing it.

**Look at the blue one. Paying attention to tone and content**
**Who do you think this one is for? Who might respond to such a message?**

F2-6 - Personally, I prefer the positive one in comparison of the two. It feels more attractive to me. But I can also see the value in having both. To try to convince people to try to respond. The one thing I liked better about the (wolf) was the bulleted sections. This (blue) was a bit more of a wall of text, not difficult to read at all, but it didn't highlight it as well as the format of the other one.

F2-5 - Phishing emails don't scare me. It's the second part, that's most important and by the time I got to that my eyes were kind of glazed over. I was like, Oh! I can skip this part. I mean, I read all of it for the sake of the focus group, but if I were encountering this, I wouldn't even get to the second paragraph. I understand phishing emails and I get how that works.

F2-3 - I appreciated that this pointed out how the phishing emails look like authentic emails because if you've been using email online you're like, Oh! I know what they look like. Mmm? They've gotten better. They've gotten harder to discern.

F2-5 - But the context. If someone you know asks for your password or vulnerable information over email, that usually triggers…

F2-3 - Right! But that's not always what happens. Like recently the thing where we sign into your Google Drive. That's where it happens and that's the sophistication that people may not realize.

F2-2 - Not send me your password, but…

F2-3 - Yeah!

F2-1 - It's happened to me a few times. My email, from my email, my whole contact list gets a "click this link" subject line and there's a link. Most people know…

F2-5 - "Don't click on it."

F2-6 - But they know I didn't say that. But my grandma might not know. I don't know what happens once you click on it.

F2-6 - kind of unrelated to this, but something people could do that people aren't aware of is reading the email headers to be suspicious about things. But I don't think very people know how to do that. To get who the real sender was. I think on that it said, it who it came from.

**But the "to" said hhhhhh**

F2-6 - and many times it will say amazon.com but if you look at the headers and it's from something dot ru or something.

F2-3 - I appreciated that this said that U of M offers a free service. It's a little thing, but everybody loves free stuff.

F2-5 - And the U cares about me.

F2-3 - Yeah. Yeah. and like with Duo, you can make a difference. Like we're in this together.

F2-2 - I even thought that could be like a "U"

F2-3 - And then it's like "take 10 minutes with your device and your computer...blah, blah, blah and you'll feel great knowing that...it talks about how you'll feel after you're doing it. And I appreciated the if-then statement. If your password is stolen then access to your accounts is just a few clicks away. So, it gives shortened consequences.

F2-4 - What I didn't like so much about the second one is that the first one had a very nice story all through the components and then it had the thing to do. In the blue one, there a thing about phishing is bad, and if your password is stolen, so it's like how did we get to the point where it's

me somehow clicking on an email and suddenly my password is stolen. I'd like that explained. How have I given out my password?

F2-2 - I had a similar thought. Like, I know that, but the connection of phishing email, what did I do to the phishing email?

F2-4 - Exactly.

F2-2 - I clicked on something…

**If you had to compare the two, which do think would be more motivating for you or people you know?**

F2-1 - I think a mix of the two. I like the friendlier tone and the if then statement. From a marketing perspective, you need to have the bullets you need to have "ten minutes" things that just (snaps) because people aren't gonna read this.

**So, if it were a more positive tone with more bullets, that would sweet spot.**

F2-1 - The clear story with the marketing visuals, I think that one.

F2-3 - I really like logo continuity. Because a visual of what Duo looks like, when I go to the z link, oh okay, this looks the same as it did on the poster. I mean everyone likes a smiling woman, but…

F2-4 - She's having way too much fun with it.

F2-6 - I know! I need a computer like that!

F2-4 - If work was like this all day.

F2-3 - The point here is protecting yourself from identity theft, but really the point is Duo Protection, to get you to get that little green app, yeah.

F2-6 - I agree. I think a mix would be ideal for me. This image (blue) and these bullet points (wolf) and either content works well. I'm not big on marketing generally, but I do like the University colors, instead of the blue. It seems more official.

F2-5 - This seems more like an ad to rent like an apartment. She's feeling great about it.

F2-2 - Were you logging in securely on graphic stock?

**Your advice**

F2-3 - I think it comes back to stories. Stories that I heard on reply all were super compelling, the stories I heard in the workshop. It made it real and it kept my interest from beginning to end. It's

a little bit harder to market and a little bit harder to say like Listen to this two part podcast episode. I promise you'll love it. And I'll say whatever...I don't listen to podcasts.

F2-1 - That's why podcasts are gaining popularity because they use really intimate stories that talk to a lot of people. You can see yourself as a person who got hacked or whatever because the way you listen to it. When you're inundated with messaging in our email or our homes or whatever, you're gonna get an email and just delete it. If there were something like Lauren over at Northrup, or there was something to kind of pull you in.

**The only problem with that is that we really don't want to shame people.We've all fallen for it and felt like "that was me." We could do fictional…**

**Listening to the podcast...if we promoted those, would anyone listen to one?**

F2-2 - I did listen to one about the FCC and net neutrality, so maybe.

**Part of it is that you have to catch people where they are with messaging they want to hear, so where are some of the place you go.**

F2-3 - I usually skim through the U of M Brief

F2-2 - I think most people in my office read the Brief.

**We had a safe computing campaign have any of you noticed it, or clicked on it.**

F2-2 - I think I've noticed it, I don't know that I've clicked on it.

F2-4 - Is that related to Duo?

**We did one month about 2 factor in general, but Duo was a separate email campaign.**

F2-3 - I also get the campus climate digest. I skim through that. It's about student and employee safety.

F2-2 - I don't know about reaching students, I know it's a struggle. But thinking about my department, if that was a message that I could bring to our staff meeting, have you noticed this...just to have it come up in actual real-person conversation to raise people's awareness. Because you see it in email you see it in email, but just to encourage at the leadership or director level.

F2-5 - How about safe computing ambassadors in different areas?

F2-1 - We've talked about that here, because we have an emergency plan for active shooter, or weather. But do people actually know what to do because it's a sheet on a wall and do you read it through...or if you're new. So, I was like, once a year, or once a semester at the staff meeting, talk about the emergency plan. Could you do it here so that once a year or when they're new, they hear about safe computing. The more you talk about it.

F2-5 - Or make it mandatory. If you want to use direct deposit anymore, you have to have Duo. You have to, to get into Peoplesoft, why not.

F2-6 - Yeah, and you have to have a password, so it's arguable.

**I think someday it's possible. Other institutions have done that and have done it at the log-in level.**

**The positive message felt better, but the wolf has more urgency. Yes?**

Yes.

## Focus Group 3

### *Participants*

| Focus group 3 member identifier | Age range | Gender | Education | Marital status? | Ethnicity | Familiar with term "safe computing?" | Have you ever received a phishing email | Has your password, credit card number, bank account number, or social security number ever been stolen? | What is your level of concern re: cyber crime | Probable victim of cybercrime? |
|---|---|---|---|---|---|---|---|---|---|---|
| F3-1 | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported |
| F3-2 | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported |
| F3-3 | 35 - 44 | Male | 4-year degree | Married | White | Yes | Yes | Yes | Slightly concerned | Neutral |
| F3-4 | 35 - 44 | Female | 4-year degree | Never married | White | No | Yes | No | Moderately concerned | Not probable |
| F3-5 | 35 - 44 | Female | 4-year degree | Married | White | Yes | Yes | Yes | Moderately concerned | Somewhat probable |
| F3-6 | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported | Not reported |

### *Notes*

**What are some of the words and feelings that come to mind when you hear the term safe computing?**

F3-5 - Virus

F3-6 – Malware

F3-2 - Identity theft

F3-4 - Smart choices

F3-1 - Tiring. Having to keep up

F3-5 - Vigilant

F3-6 – anxiety

F3-4 – fear

F3-2 - Mixed feelings. Disappointment that you can't just...always have to be vigilant

F3-5 - maybe even a little embarrassment, or the threat of embarrassment. You'd be seen as incompetent possibly even if people say, oh yes. You think that won't happen to me. I won't fall for that.

F3-2 - Anger if anybody takes advantage of you that way.

**Do you all talk about safe computing with your colleagues, do you know what they do or what practices they have?**

F3-6 - We've talked about it as a staff with regards to the VPN when you're traveling and that even if we're working from home, if we're doing any, like checking our email or anything like that.

F3-5 - We are a very active department on slack. So, if anybody sees something come through…something they got...they will share it on slack and it will quickly be read because we're very active on it. So, it's a support system. Other than that, everyone gets the emails because we work with IT closely so we see the emails and I would think most of us think we're experts on it even if that is a misconception

F3-4 -I don't think we talk about it. I mean I've made comments about my coworkers' passwords being a million miles long you know, but it's not like something...we don't talk about smart ways to format passwords or...we are involved in a lot of security with keys, because we manage a lot of space and it's all in lock boxes and things like that um but just logging into the U. It's not something we talk about. We get the IT stuff. But we don't talk about it.

**What about with the recent Google Drive scam?**

F3-4 - So when those come in, I'm like what the heck. But we don't...we naturally just don't agree to that. If I don't know who the person is, I'm not just going to agree to that. If I did know them...but then it immediately came around. It said it was phishing, mark it as phishing and this is how you do that. You know so there was a notification. We didn't talk about it with one another.

F3-1 - In our office we have half-height cubes so it's kind of like a gopher town where people pop up and say, "Hey, did you see this?" Within five minutes everyone was trying to figure out where is it coming from. We're a consulting service for faculty and we were getting them from a

lot of faculty accounts and we were trying to figure out what was going on and about 15 minutes later the email announcement came out to not click on those. So, we were just trying to figure out what was going on.

F3-2 - For me, this is as of late been an express part of my job. We were asked to put down ideas that we could communicate to OIT. What are some of the best practices? What are some of the things we should be doing and more specifically password management in the data warehouse group where we have a lot of important passwords and if we're sharing them we need. So, we're working with that group as just a regular part of my job.

**So, what about with your friends and family? People are concerned about the elderly.**

F3-5 - My parents are not online for email. So that is not an issue.

F3-1 - Mine are. I worry about it all the time especially since they really embrace trying to do their banking and retirement accounts all online. I know that their tech literacy isn't that great so I worry about them getting in trouble that way.

F3-4 - My mom's computer is full of some viruses. It keeps telling her that she needs to contact somebody for help but she's like "I don't have time for that." and so she doesn't. I'm like mom, don't!"

F3-6 – But, that could probably be a scam too.

F3-4 - It is, but she's like I don't have time for that. I'm like you get that fixed. You interact with things on Facebook through your email. You don't even know how to like things on Facebook, you don't even go to the site. Do not buy any virus software, wait 'til I get there. She's scared enough that she doesn't just do stuff. But people get confused pretty easily.

F3-2 - We've had a couple of discussion in my home. Just my wife and I. She's got the tape over the camera on her laptop. She made sure that when we had the x box, she turned the camera. She's very sensitive about that. I've gotten into smart-home automation with sensors that can tell when you're there... She's very leery of it. She wonders if someone is going to hack us. She's much more privacy averse about some of these technologies and what might happen. I understand the tech. I should be able to know when I can and can't do things, but I would say she's the more nervous of the two.

F3-4 - I think I've only had one conversation with my parents about safe computing. My mom used to work at a university, and when she was getting it set up she took it to a tech at the U, so she knew it was all set up with all the good virus software and the set-up is good to go. My dad is a little less computer savvy than my mom. But she would tell him if he were doing something wrong.

**What are some of the way you or your colleagues learn about scams. Do you know what's the latest in password creation?**

F3-6 - I depend on emails from OIT and safe computing. If something pops up, I don't want to say on Facebook, but somewhere online...I don't know what it the Google stuff that rose high enough in the news that it was actually covered?

F3-4 - I think so. I think I shared an article on Facebook

F3-5 - Yeah. So, some of the communities of practice and the Google groups as well.

**Are there are any safe computing behaviors that you know you should be doing, but you don't do?**

F3-1 - I do have the Duo turned on for, I guess, the W-2, but I tried it for the general log ins, but it just got in the way so much, particularly when the wireless network was being upgraded and it was getting in the way of things and I would have to walk to another building to log in. So, then I ended up disabling that, but I still have it for W-2 and direct deposit.

**So, when it is more inconvenient than you think it's worth, you don't practice the behavior.**

F3-2 - I know I don't use as many passwords as I should. I kind of got in the habit of using a simple pattern. I kind of thing oh no one will figure that out. But it's too short and I know that's part of the problem.

F3-5- I have a stable of passwords that I use. So that one didn't work, well maybe this one will work. I know that's not great, but I don't care. I can only remember so many things. And then I

also use the practice, that I keep some of my passwords on my phone, which is password protected. But MyMedica, I'm never going to remember what MyMedica password is or all these things I have to keep track of.

F3-3 - I reuse my passwords a lot.

F3-6 - I reuse my passwords all the time.

F3-4 - I reuse my passwords, some of them. And they've talked this, about how even minor applications are starting to collect data on you that if you have...it's not just your email anymore, it's like signing up to go whatever it is...you know for the American Red Cross or donating money to whatever campaign, and if you're using the same passwords there that you are on your email, or in various things they can break those and then go after other stuff. Um... someone suggested a thing called password safe which is where you can keep a list of all of your passwords.

F3-2 It's an app. Lastpass is the one the U settled on.

F3-4 - Yeah. But I haven't used that yet, so I'm still not safe.

**What do you think are the consequences? What could happen?**

F3-5 - A lot of the time, I don't care what people see on mine. I'm not putting things on Facebook. Everything is public facing. I never have anything on there that I wouldn't want everyone seeing. When it comes to banking, I know my bank will refund me. It will be thoroughly annoying, if someone hacks it, but I'll get my money back. So, consequences wouldn't be dire.

F3-4 - They are starting to create fake people. They are starting to collect behavior of people and information from various people and creating personas that then pretend to be a real person and do things. Specifically, steal your medical card numbers and then go get treatment off of your insurance and stuff like that and so it's a little. Like hunh. How to. I opted into an identity protection service, so I feel okay about that, but a lot of people don't.

F3-5 And do you pay for that service?

F3- 4 - $8 per month for that service. But I have had my email password, and then they start sending email out of my account and then I'm blocked. So, when I try to send legitimate emails to people I know, I'm suddenly in the junk box. And that's been annoying. I've also had people sign me up for stuff using my other account which is annoying. They were signing me up for Fingerhut and pink and anything I did not have an account on, they were trying to sign me up. I'm like why are they doing this? Why am I being signed up for eBay using my email? What the hell are they going to do? And I contact these companies and I say this is fake. I don't want an account with you. I don't know who is doing this or why. It's just weird. I'm just like why is this happening.

**So, annoying things?**

F3-5 Yeah.

F3-2 - I'm probably most concerned about financial things. My wife's somehow...it had to do with her SSN being very similar got confused on the credit rating systems. Hers and another person. The names were different. All of a sudden, these bad credit things from this other person were affecting her. It took years to try and figure it out.

F3-6 - That makes me nervous. The whole credit reporting because that can affect so many parts of your life. If you want to buy a house or a car or something. And if you're trying to get your credit report all cleaned up, I heard it takes forever. I'm like you call and nobody cares.

F3-5 - And that costs you real money. You get a higher rate for your car loans or your credit cards. Whether or not you get that mortgage.

**Other consequences**

F3-5 - It rarely crosses my mind, but that someone could track where I'm at. But again, you can google me and find out where my house is if someone really wants to find me. I take the attitude that I'm not that special. Or if they really want me, they're going to get me, so whatever. But I

thought about people who do crimes but they take their phones with them. I'm like you guys, don't take your phone with you. They can track your GPS.

F3-1 - I guess I share a little bit of that feeling of inevitability. It's just trying to make it hard enough for someone to steal my identity so maybe they'll go after someone else. It's not a very charitable thing to do to the rest of society, but I don't really know what else I can do.

F3-6 - Occasionally, I'll do a Google search of myself just to make sure that everything is okay, if there is something weird floating out there. I have found my own age, address and phone number. And I think how do I get that to be not quite so readily available?

F3-4 - Public records.

F3-6 - I know! Public records. But it used to be that you had to send a written request to the records office and three weeks later, they'd send it back to you.

F3-5 - But, you used to also be able to go to the DMV and ask for someone's address. You used to be able to do that before stalking laws. You know so we just keep going down this path.

F3-6 - Also, I'm guilty of this, but I post pictures of my child on Facebook. I've often seen articles about how you really shouldn't do that. But everybody does it.

F3-5 - I don't post other people's children. But I'll share my own. But I'll make sure they're not taggable and all that stuff.

F3-6 - Or don't checking in at the middle school.

F3-5 - Oh yeah! Or even with the pictures for the first day of school I make sure I don't get the school's name in the photo.

F3-2 - Again, the location is probably in the metadata

F3-5 - Yep. Again, if someone really wants it. But then I remind myself that we're not any more unsafe than we were 40 years ago. We just all know about it now immediately. I try not to live in fear.

F3-3 - I can't believe that there aren't more services that are using two factor. I can't believe that Facebook hasn't adopted 2-factor.

F3-1 - They have it, but they don't require it.

F3-3 - Do they have that capability? I didn't know

F3-2 - I'll sign up for that.

F3-3 - I have 2-factor at the U and turned on for my personal google account. I also used to work in identity management, so. It adds such a huge dimension of security to your account, I can't imagine why you wouldn't do it. Except for the convenience factor. And I think that once you have it and understand the implications of not having it, it seems like such a no-brainer. I wish...banks are starting to do it. I wish my credit union would.

**So, the safe computing behaviors that you use, how confident are you that they'll have the desired effect, that they'll keep you safe?**

F3-5 - I think they are better than nothing, but I think it's a matter of time until they break that one, and you just kind of stay ahead of it. I don't think that anything is perfect.

F3-1- I feel the same way. I've read a few news reports of celebrities who have had their two-factor subverted somehow by people who manage to impersonate them and steal their phone number in order to break into their accounts. I figure it's only a matter of time until that works its way down to the rest of the population. I've talked with T-Mobile and the info that they ask when you call in is pretty minimal that you might be able to find out if you Google me and so its

F3-5 - Or a family member who is the person most likely to steal your identity or someone you know, right?

F3-2 – Yeah, I think you take precautions and you think "I probably could do more." Part of me tells myself unless someone has a reason to target me, I'm one of billions of people that they could go at. So, I'll take my chances. I know that's sort of a false sense. My brain says that a

false reason, but at the same time, it probably explains why I put the level of effort that I do, but not more. It's that I take some of the obvious steps, but don't go too far with this.

**And it's kind of an arms race?**

F3- 2 - If I had something that was so valuable to protect, I would lock it with a lock that was like $10 then eventually, when it's worth more than $10 it's gonna be worth it for them to go get it. It's the same thing for me. I think of cyber security pretty similarly to physical security. If it's not worth a lot you don't have to spend a lot of time and energy on it. If it's worth a lot to you and the loss and inconvenience would be you know great, then you spend more time and energy on it. So, the financial stuff and medical are the ones where I try to be a little bit more secure and the social stuff I don't put as much value or effort on.

**And what about U data. If someone gets access to your account, would they also be able to get access to sensitive data?**

F3-2 – Yeah, they would. It's part of our job to manage that data. We're trusted with that. So, I protect those with more cognizance than I would my Facebook account.

F3-5 - I literally work on communications so everything I have would be...the aim is to be public. They can get some back and forth comments from people on what we want to say, but no access to sensitive data.

F3-6 - I don't have access to sensitive data

F3-4 - I have access to student records in Peoplesoft, so that's all kinds of information, up to and including grades and stuff like that. I don't go there. I'm not interested. We have Duo. that is what OIT says to do.

F3-1 - I have admin rights to our LMS which means that I have access to the student IDs, grades, assignments, faculty members accounts, all of that. I can pretend to be them. So, our group has adopted Duo for any of our admin functions as an extra precaution.

**Re: Wolf - messaging around safe computing: How does it make you feel? What are your reactions?**

F3-5 - I'd just say, require it. When it is something that rises to this level of importance, make it mandatory. I know that U does not like to do that.

F3-5 - What if people don't have a smartphone though?

**You can use your desk phone, if you have a desk phone. You can also use a nonsmart phone. They have fobs as well.**

F3-2 - I thought the maroon and gold colors were playing positively on --part of the U, you know University pride, loyalty, honor. The maroon and gold is always like "Rah." From an emotional standpoint, it got me thinking, do the right thing for the University as well as University pride.

F3-5 - Like the herd mentality that you get for the flu shots. Like we're the herd. The U is the herd. Do it for the herd.

F3-6 - I thought the text struck a nice balance between not being overly dramatic..it's has a sense of urgency but doesn't seem to be going into the "sky is falling" The way that the vocabulary was used, not too dramatic not too wishy-washy.

F3-3 - It's a sobering tone, but it's also a little overwhelming. I think that the image is pretty stark and kind of scary. It's not necessarily a criticism, it's hard to scan, it's hard for me to pick out what am I supposed to do and the image is just so...my eye is so drawn to the image that everything else just kind of fades away. And I'm just kinda left being scared.

F3-1 - I have to admit that people like you fall prey to ...put me on the defensive. Would they really get me?

F3-6 - They would totally get me. We just have to outrun you, right? The wolves?

F3-3 - Right. You only have to be faster than the person next to you.

F3-5 - I think it did give you steps. You could walk away and you have steps to do it today. There's a call to action.

F3-2 – Yeah, there's a call to action.

F3-6 – But, it's text heavy.

F3-2 – Yeah, a lot of words, and the smaller font type is maybe. Maybe bullets instead. I like, when you were mentioning that it's not too out there, the words are strong, but there are no exclamation points which softened it enough. I was looking, when you read the words it's pretty strong. But it didn't hit me.

F3-5 - They weren't underlined and exclamations

F3-2 - Right, just the graphic

F3-6 - And we all know this. We are all targets for identity theft so I didn't feel like this..like you said, without the exclamation points, yes we are kind of targets for identity theft.

F3-3 - Not me.

F3-4 - I would suggest putting the bottom line up front and the bottom line isn't convincing people that they are targets, it's that there is duo protection, use it. Because you'll get people to here and then you'll lose them. I think it's fine to have the phishing emails are like wolves, not above stop criminals from getting your SSN and paycheck because I think that's the message here. Use Duo.

**What about the tone for you?**

F3-4 - The tone is conversational, which I like. But people don't read anymore.

F3-2 - Yeah. They skim.

F3-4 - I mean you tell them directly and exactly what they need to know, and they say, "You didn't tell me that, and I'm like, "Yes, I did." But they didn't read it. I didn't think it was overly in your face like you better do duo now or else...it wasn't like the boogeyman is coming to get you. It wasn't like that. But it wasn't...well it would be nice if you would. It was pretty direct. Stop criminals from stealing your stuff: do this this thing.

**Were you aware that one of the reasons is to protect your paycheck.**

(nods all around)

F3-5 - They also made a big push during tax returns.

**RE: Blue rational-confidence building messages**

F3-6 - I don't think the call to action was strong enough. You can help protect. I would go "protect your identity" to me it looked like a banking poster. And again way too much text. And too much information. "You'll feel great knowing" Don't tell me I'll feel great. Just 10 minutes, two ways to protect you.

**So, it's not really easy, so we don't promise it. It's ten steps. Some novices had never used a QR code and it takes ten minutes.**

F3-2 - The set-up is not easy, but the use of it on a daily basis is easy especially if you can get the push to work. At first push didn't work for me. I redid my phone and now it's a piece of cake. The blue color and the smiling faces. It didn't seem like it was telling me about theft, it seemed like it was telling me about something happy. So, I was a little confused by the messages.

F3-5 - Is it the thief who got in?

F3-3 - No. She's not wearing stripes. She doesn't have a mask on.

F3-3 - I think this one is actually easier to scan. It may or may not have the same amount of text. But I feel like it's easier to find the most important things. That being that Duo and you can make a difference and the thing about what 2 factor auth is. I read the call to action as the sign up today for Duo Protection. I felt like that was a lot clearer in this one. The rest of the image was easier to ignore. It looks like it could be an ad for MyMedica or something like that. I'm going to sign up for my doctor's patient portal or something like that. That's kind of how it looks to me.

**Does it seem like something you can ignore?**

F3-1 - I feel like what I'm supposed to do is buried in the text. So, cutting down on the text. Maybe a diagram to show password plus phone to login to sort of explain what it is without a paragraph of text.

F3-3 - I feel like this doesn't totally get me there. I feel like the information of what I'm supposed to do is easier to find, and I don't feel like I'm being pushed as hard, or manipulated or made to feel scared by the way the message is being presented.

F3-6 - It has more of a tone like I'm your friend, I'm telling you what you should do. Duo is now my best friend because now we're together. And we're so happy in this picture. This lady is way too happy.

F3-3 - She has that blissed out like, "I just signed up for two factor auth" I've seen that a few times during my work with IDM. I mean let me tell you, when you see that expression on a customer's face...it just makes all the work worthwhile.

F3-6 - But it is less anxiety inducing than the whole scary wolf in sheep's clothing one.

F3-5 - Is this more carrot and the other one stick?

**What makes you more comfortable? Do you want more urgency or comfort and confidence-building? Both? What would motivate you?**

F3-6 - I actually think the fear one. I don't know for me personally, it seemed much more important that I do it after I read the wolf one.

F3-5 - Or "You will stop being paid if you don't do it by x date"

F3-1 - I respond more to an emphasis on consequences. Like what could someone do if they get your paycheck.

F3-1 - Or your body will be hollowed out and occupied by a predator.

F3-2 - I wrote that down. That the wolf was more motivating, but as I sat and listened to carrot and stick and stuff like that. This is a little disturbing (the wolf). This (blue one) is obviously more pleasant. I don't know. I'm thinking I would more likely ignore this (blue one) but I feel better about it. Hahaha!

F3-4 - I like the blue one better, but I'd probably be more likely to do something based on this one.

F3-6 - With the blue, it seems like this is a great idea for you…

F3-5 - Yeah, and I'll get to it never

F3-5 - Don't come crying to us when your identity gets stolen…

F3-3 - I don't feel particularly motivated by either message. This one feels like trying too hard to scare me. I hope you didn't make this one. The design doesn't feel as professional...because I'm uptight it offends me. The blue one stresses me out less, and I don't like being stressed out.

F3-5 - But will it make you act?

F3-3 - It's hard for me to say cause I've already done it. I use it whenever I can. I'm already sold on this. But I feel like this message, it's easier for me to find what's important and that goes a long way for me personally.

**If you were to tell your neighbor…**

F3-5 -I'd use both. I think they can take it.

F3-1 - Teenagers think they're invincible. I'm not sure if that would appeal to them.

F3- 5 - Some people would be overwhelmed? While digital natives wouldn't be.

**What kind of message would a millennial respond to?**

F3-3 - I think millennials would respond to blue one more. They are more sophisticated consumers and they are so used to being targets, that they will see right through to the tactic and think you're trying to scare me into doing something. The softer approach that is less manipulative would be more appreciated by the younger folk.

**Advice for safe computing in general**

F3-3 - There is going to be so much research about messaging and tone after this election, that especially along the lines of fear-based messaging

F3-6 - And maybe some backlash from people who realize they're being manipulated

F3-2 - It can't be overly strong with fear. I think it needs to be educational. Your facts are about bad things. Not we're trying to scare you.

F3-3 - I think over the long term...I think fear can be used to motivate initially, but if the fear overtakes the information you're trying to convey, because this is an arms race, and I think that personally if I'm getting bombarded by big scary messages, then I'm gonna step back.

F3-4 - I'd say storytelling is your best choice. Not just long hard...8 million is lost every year, not that kind of data,

**But, John, guy down the hall**

F3-4 - Yeah.

F3-3 - Understanding that this is a tool, it's not the only tool. It's not that if you don't do this, the world isn't going to fall apart. This is something that is important to do because of...there's underlying threat. And it's understanding that there is a threat that I think is going to be better over the long term.

F3-1 - I tend to agree with [focus group member 6], when she said just make it mandatory. If it's just part of signing up for your account. Then we don't have to worry about the messaging. This is how the U of M works.

F3-2 - Matter of fact.

F3-5 - It helps protect you

**But, for safe computing in general, how would you advise me to help people learn about. We've done a safe computing campaign about specific.**

F3-5 - If you could find a student who could talk about how it messed up their life or something. If there's a faculty member, that would go further with other faculty. Like if my research was...it's got to be their audience.

F3-3 - Somebody else already mentioned it, the do it for the herd. Like for the flu shot. The message, but also going to people around campus. So, like why not a campaign. We'll come to your building. You'll walk in, five minutes later you'll walk out with your account more secure.

F3-5 - We'll come to your building.

F3-3 In the past when it came to flu shots, I thought I'm young I'm healthy dude. I eat healthy, I exercise a lot I don't get sick I'm not going to do it. I think part of the reason why I changed my

mind was that campaign. That it wasn't just about me. I mean, I may get sick for a day, but during that time, I may make 5 other people sick or something.

F3-1 - Setting it up in dorm rooms. If someone is in the lobby with a computer, that teaches people that if someone is sitting down in the lobby, oh my gosh that's bad behavior.

F3-2 - If we can change the mindset that more people are doing it than not, people want to be part of the group. They want to be part of the larger group. Once we get the ground swell…

Part of what I was talking about it. How do you know it's the social norm if it's just something you do at your computer...you won't believe it, but I reset my password today!